Privacy e cyber security in Sanità.

Massimo Montanile[1]

La Sanità sta soffrendo la sua scarsa capacità di adattarsi ai profondi e veloci mutamenti indotti dalla trasformazione digitale. Al di là di alcune eccellenze, lo stato della Sanità in Italia impone urgenti interventi per rimuovere le cause radice che ancora oggi ne ostacolano l'evoluzione verso modelli in grado di affrontare le nuove sfide. In questo capitolo proponiamo una lettura della situazione italiana della Sanità relativamente alla privacy e alla cyber security, attraverso l'analisi dei provvedimenti dell'autorità Garante per la protezione dei dati personali[2] , del report predisposto da AGID[3] "La Spesa ICT 2021 nella PA italiana - Principali trend e percorsi in atto" e del White Paper "Capire Il Rischio Cyber Il Nuovo Orizzonte In Sanità", pubblicato a luglio dello scorso anno da Sham e Università di Torino - Dipartimento di Management.

Sanità e privacy

Ogni anno il Garante privacy pubblica la Relazione sulle attività svolte nel corso dell'anno precedente. Nella Relazione presentata lo scorso 2 luglio, l'autorità per la protezione dei dati personali[4] ha denunciato di aver ricevuto, nell'anno 2020, numerosi reclami e segnalazioni in merito al trattamento dei dati personali effettuati da parte delle strutture sanitarie, soprattutto nell'ambito della gestione dell'emergenza sanitaria (circa 150), spesso per grossolani errori di comunicazione[5].

Nel settore della Sanità il Garante ha svolto, nel 2020, un'intensa attività intervenendo a dare chiarimenti e prescrizioni a medici, strutture sanitarie e soggetti privati, sul corretto trattamento dei dati dei pazienti.

Relativamente al Fascicolo Sanitario Elettronico (FSE), sono state avviate numerose istruttorie concernenti, principalmente, l'erronea attribuzione di referti e documenti sanitari in FSE di soggetti diversi dall'interessato e l'accesso al Fascicolo da parte di personale che, seppur autorizzato, non era coinvolto nel processo di cura dell'interessato.

Anche per il Dossier sanitario sono stati più volte denunciati accessi da parte di soggetti che, seppure autorizzati, non erano coinvolti nel processo di cura dell'interessato. O addirittura si sono registrati casi di accessi al dossier sanitario aziendale da parte del personale medico per "mera curiosità". Altri casi hanno riguardato il mancato oscuramento di alcuni dati e documenti a seguito di specifiche istanze presentate dagli interessati o, ancora, la presenza, nei dossier sanitari, di dati relativi alla salute di terzi.

---

[1] Data Protection Evangelist. Membro del Comitato Scientifico dell'Associazione Scientifica per la Sanità Digitale (ASSD), Membro dell'Advisory Board dell'Associazione OSINTITALIA, Fellow dell'Istituto Italiano per la Privacy e la valorizzazione dei dati (IIP), Delegato Federprivacy Città Metropolitana di Roma, co-Direttore della Collana Cyber Security Defence di tab edizioni, DPO Elettronica SPA, DPO Cy4Gate SPA.

[2] I provvedimenti analizzati sono pubblicati sul sito del Garante, url: https://www.garanteprivacy.it/home/provvedimenti-normativa/provvedimenti#layout_9599165.

[3] Il report è stato predisposto da AGID con il supporto della società NetConsulting[3], nell'ambito delle attività del progetto "Italia Login – La casa del cittadino", finanziato dal Programma Operativo Nazionale (PON) "*Governance* e Capacità Istituzionale 2014-2020", Asse 1 Azione 1.3.1. (Agenzia per l'Italia Digitale, Roma dicembre 2021).

[4] Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675). Il c.d. "Decreto di armonizzazione" (Decreto legislativo 10 agosto 2018, n. 101) ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51). L'attuale Collegio, eletto dal Parlamento il 14 luglio 2020 e insediatosi il 29 luglio 2020, è così composto: Pasquale Stanzione (Presidente); Ginevra Cerrina Feroni (Vice Presidente); Agostino Ghiglia (Componente); Guido Scorza (Componente).

[5] Le segnalazioni hanno riguardato le modalità con le quali le strutture sanitarie hanno trasmesso ai pazienti affetti da Covid-19 informazioni relative alla loro condizione attraverso l'invio di e-mail a tutti i destinatari inseriti in chiaro nel campo relativo ai destinatari, oppure trattasi di reclami relativi alla ricezione, da parte di pazienti, di referti Covid-19 riferiti ad altri soggetti, ovvero, da parte di istituzioni, di pubblicazione elenchi dei soggetti positivi, al di fuori dei casi previsti dalla legge.

Numerose infine le notifiche di data breach pervenute ai sensi dell'art. 33 del RGPD con riferimento ai trattamenti di dati personali effettuati in ambito sanitario dalle quali sono scaturite numerose istruttorie.

La situazione nel 2021 non è migliorata, anzi. Sembra assurdo, ma ancora oggi c'è chi, in Sanità, accede a software diagnostici con un'utenza di tipo amministrativo (admin) e password non robusta (admin)! Al di là del caso citato (a quanto pare molto diffuso, ahimè), sono stati analizzati i Provvedimenti dell'autorità Garante relativi a Sanità e ricerca scientifica pubblicati nel periodo 1.1.2021-25.1.2022, che hanno confermato la necessità di interventi urgenti. Si tratta di **153** provvedimenti, che in particolare hanno riguardato (cfr. Figura 2) Aziende sanitarie (30), Centri medici (3), Operatori sanitari (14), Ospedali (12).

L'analisi tipologica documentale relativa ai 4 soggetti sopra richiamati è illustrata in Figura 1, dove si evidenzia l'alto numero di ordinanze di ingiunzione (43) pubblicate dal Garante nel periodo esaminato. Le ordinanze di ingiunzione sono interessanti, poiché riportano schematicamente e in dettaglio gli aspetti di interesse per il nostro lavoro:

1. La violazione dei dati personali.
2. Esito dell'attività istruttoria.
3. Conclusioni
4. (eventualmente) Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie.

I provvedimenti del Garante in Sanità generalmente si riferiscono a violazioni di dati personali relativi alla salute, che meritano una maggiore protezione dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali (Cons. n. 51 del GDPR). Infatti la disciplina in materia di protezione dei dati personali stabilisce che i medesimi dati devono essere "*trattati in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*" (art. 5, par. 1, lett. f) del GDPR).

Per quanto riguarda la supply chain, il GDPR ha anche disciplinato gli obblighi a cui è tenuto il responsabile del trattamento e l'ambito delle relative responsabilità (v. artt. 30, 32, 33, par. 2, 82 e 83 del GDPR). Certamente sul titolare del trattamento ricade una "*responsabilità generale*" per i trattamenti posti in essere (v. art. 5, par. 2, c.d. "accountability", e 24 del GDPR), anche quando questi siano effettuati da altri soggetti "per suo conto" (Cons. n. 81, artt. 4, punto 8), e 28 del Regolamento), tuttavia l'art. 32 del GDPR stabilisce che anche il responsabile del trattamento, nell'ambito delle proprie competenze e dei compiti delegati dal titolare, deve mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (…). "Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*" (art. 32 del GDPR).

In pratica il titolare può affidare un trattamento "*a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto di misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i principi del Regolamento*", anche per la sicurezza del trattamento, tenuto conto degli specifici rischi derivanti dallo stesso (artt. 28, par. 1, 24 e 32 del Regolamento; cfr. anche Cons. n. 81). In questo caso "*i trattamenti da parte di un responsabile sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile al titolare e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del*

trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare" (art. 28, par. 3 del Regolamento).

Sanità e digital transformation

Gli investimenti ICT in Sanità sono esigui. Ciò emerge chiaramente dall'analisi del report "La Spesa ICT 2021 nella PA italiana - Principali trend e percorsi in atto" fa emergere che nel comparto ICT della PA, solamente il 4% della spesa sia destinato alla sicurezza informatica (cfr. Figura 4). Inoltre la Sanità soffre di una scomodissima eredità: il parco applicativo installato è molto datato.

Ciò comporta il continuo ricorso ad attività di manutenzione correttiva ed evolutiva, con integrazioni ad hoc, spesso non attivabili tramite l'aggiornamento delle licenze, ma solo mediante sviluppi pagati a tempo&spesa e ricorrendo a help desk specifici, innestando in tal modo il gravissimo e rischiosissimo problema del c.d. "vendor lock-in". Non solo si spendono soldi, senza alcun ritorno d'investimento e drenando risorse finanziarie a danno dei progetti più innovativi (cfr. Figura 5), si mantiene e a volte si amplia la vulnerabilità del parco applicativo rispetto ad attacchi *cyber*. Le conseguenze sono sotto gli occhi di tutti, quando l'attacco cyber viene reso pubblico…

Il rapporto SHAM, basandosi anche su fonti consolidate di riferimento per l'analisi degli incidenti di cyber sicurezza (Agenda Digitale 360 e Rapporto CLUSIT 2020), pubblicato lo scorso mese di luglio, è la prima ricerca scientifica sulla consapevolezza del rischio cyber nella sanità italiana. Un'analisi nata dalla collaborazione tra Sham e il Dipartimento di Management dell'Università di Torino. Il sondaggio ha visto la partecipazione di referenti della Direzione Sanitaria e Generale di professionisti sanitari (Risk Manager, Responsabili Qualità, DPO, CISO, Responsabili dell'Ingegneria Clinica), operanti in strutture (70% pubbliche; 30% private) distribuite su 14 Regioni italiane. Qui si riportano le evidenze più interessanti per il nostro lavoro, ma si rimanda al white paper[6] per una lettura più esaustiva dell'argomento. Il white paper è molto interessante perché restituisce una lettura del fenomeno dall'interno e dimostra la forte richiesta di investire sul tema della consapevolezza e, soprattutto, della formazione, ma anche sull'aggiornamento tecnologico. La consapevolezza, generica ma diffusa, dell'esistenza di un rischio cyber non è però accompagnata da una adeguata conoscenza dei rischi reali che possono presentarsi. (Cfr. Figura 5). Insomma solo una sanità sicura può sperare di essere digitale!

Conclusioni

Emerge un quadro preoccupante ma anche la chiara indicazione, a mio avviso, delle aree di intervento, che in sintesi possono essere:

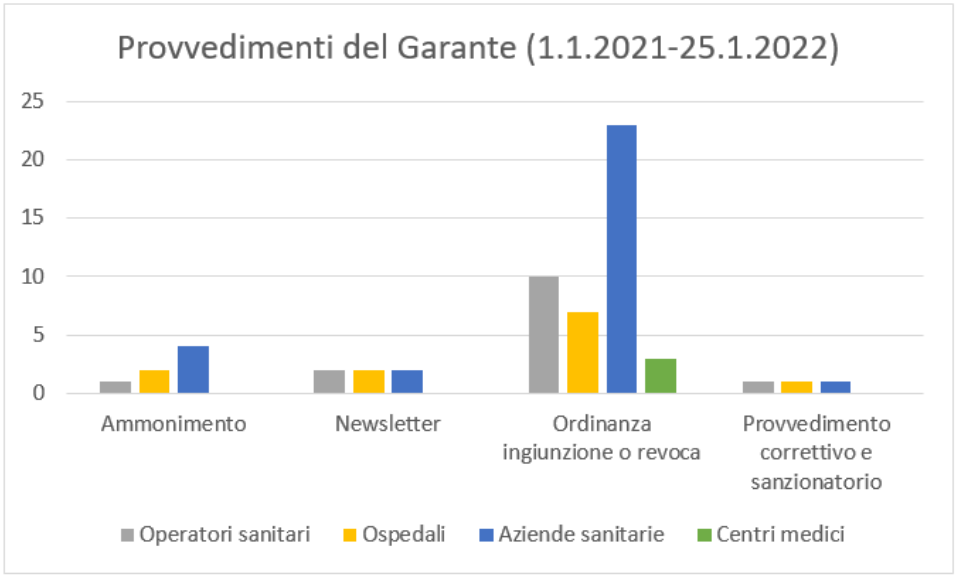
1. Rinnovare la classe dirigente della Sanità, in particolare i decisori. Oltre le consuete capacità manageriali è necessario che i nuovi manager abbiano piena contezza dei rischi e delle opportunità insite nella trasformazione digitale (in particolare privacy, cyber security, nuove tecnologie);
2. Formare una consapevolezza, diffusa a tutti i livelli ed estesa a tutti gli operatori del comparto Sanità, sui rischi e sulle opportunità della trasformazione digitale (in particolare privacy, cyber security, nuove tecnologie);
3. Gestire efficacemente la supply chain;
4. Sostenere il cambiamento con investimenti adeguati.

[6] Sham e Università di Torino - Dipartimento di Management, "Capire Il Rischio Cyber Il Nuovo Orizzonte In Sanità", 7.7.2021, https://www.sham.com/it/Comunicazione/Comunicati-stampa/SHAM-E-UNIVERSITA-DI-TORINO-PUBBLICANO-I-RISULTATI-DELLA-SURVEY-SULLO-STATO-DELL-ARTE-DEL-RISCHIO-CYBER-NEL-COMPARTO-SALUTE

Figure

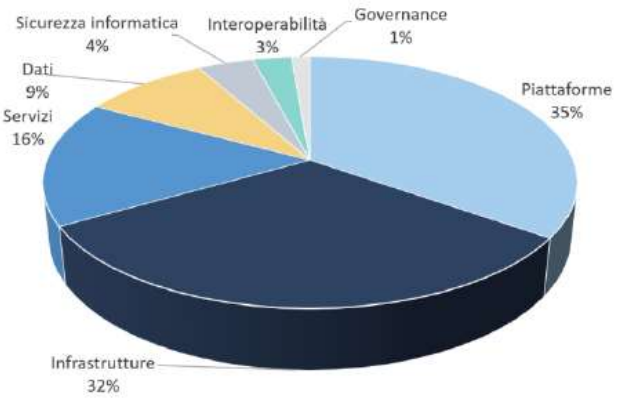
	Periodo di analisi: 1.1.2021 - 25.1.2022		Provvedimenti pubblicati sul sito del Garante: 10.845, di cui 335 relativi a Sanità e ricerca scientifica (dati al 25.1.2022) Provvedimenti relativi a Sanità e ricerca scientifica pubblicati nel periodo analizzato (1.1.2021-25.1.2022): 153						
	Sanità e ricerca scientifica (153 documenti non monotematici)								
Argomenti trattati	**Aziende sanitarie**	**Centri medici**	**Coronavirus**	**Marketing sanitario**	**Operatori sanitari**	**Ospedali**	**Pazienti**	**Sperimentazione di farmaci**	**Studi epidemiologici**
Numero provvedimenti	**30**	**3**	**93**	**1**	**14**	**12**	**28**	**1**	**3**

Figura 1 - Provvedimenti relativi a Sanità e ricerca scientifica pubblicati dal Garante dal primo gennaio 2021 al 25 gennaio 2022.



Periodo di analisi: 1.1.2021 - 25.1.2022	**Documenti pubblicati sul sito del Garante nel periodo di analisi: 880**			
Tipologia	Operatori sanitari	Ospedali	Aziende sanitarie	Centri medici
Ammonimento	1	2	4	0
Newsletter	2	2	2	0
Ordinanza ingiunzione o revoca	10	7	23	3
Provvedimento correttivo e sanzionatorio	1	1	1	0
Totale documenti	**14**	**12**	**30**	**3**

Figura 2 - Provvedimenti del Garante in Sanità



Macro ambiti PT	Importo complessivo triennio 2020-2022 (€)	N. Progetti
Piattaforme	1.176.003.709	216
Infrastrutture	1.082.169.027	102
Servizi	545.631.826	164
Dati	305.681.840	113
Sicurezza informatica	135.949.168	27
Interoperabilità	93.402.119	39
Governance	45.402.393	18
Totale complessivo	**3.384.240.082**	**679**

Figura 3 - Distribuzione degli importi dei progetti ICT nella PA - triennio 2020-2022. La figura è tratta dal report "La Spesa ICT 2021 nella PA italiana - Principali trend e percorsi in atto", Agenzia per l'Italia Digitale, Roma, Dicembre 2021.

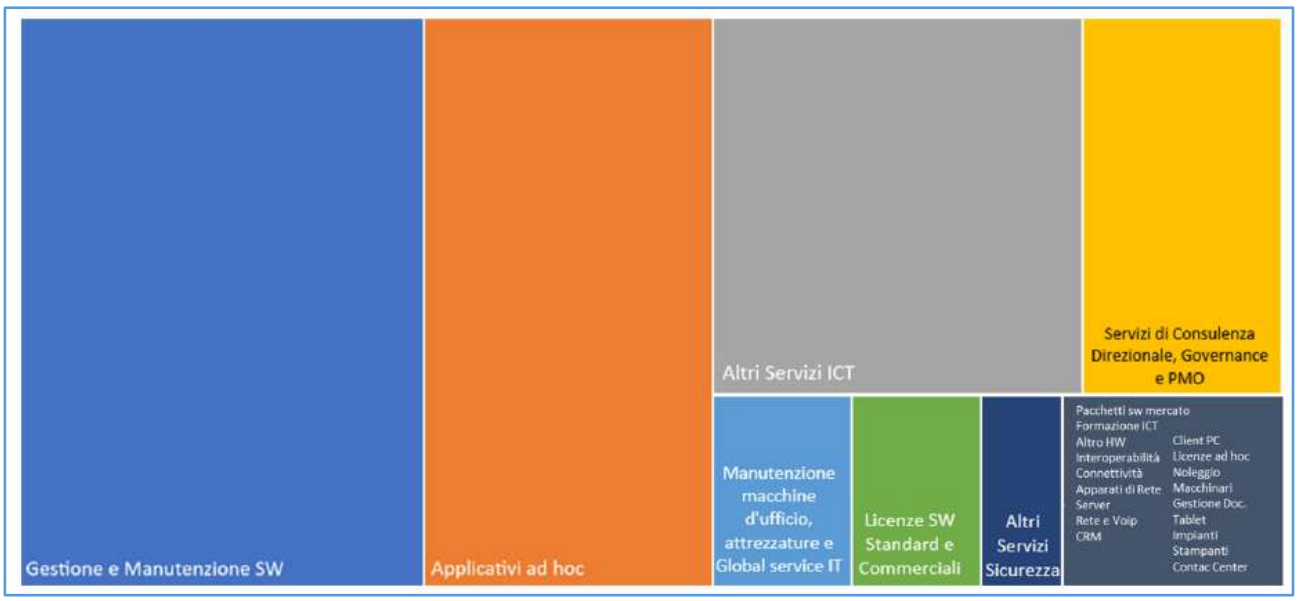


Figura 4 - Incidenza delle voci di spesa sul totale 2019-2022P – Sanità. La figura è tratta dal report "La Spesa ICT 2021 nella PA italiana - Principali trend e percorsi in atto", Agenzia per l'Italia Digitale, Roma, Dicembre 2021.

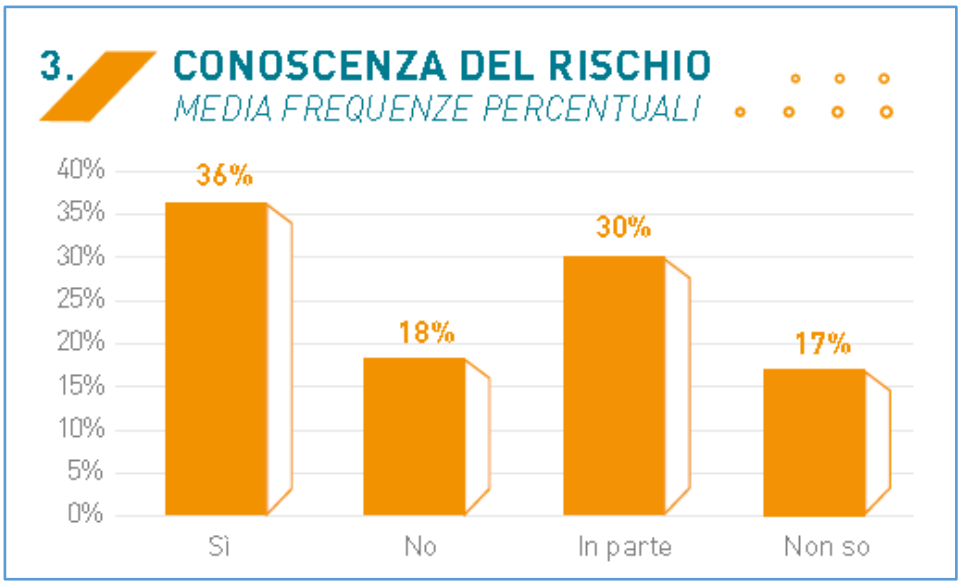


Figura 5 - La conoscenza del rischio cyber in sanita. Fonte: White paper SHAM - Università di Torino