WHITE
PAPER

ICT Security MAGAZINE

LA CYBERCRIMINALITÀ NEL SETTORE SANITARIO

ANAMNESI, DIAGNOSI E PROGNOSI DI UNA "PATOLOGIA" INFORMATICA

A cura di
MARIA VITTORIA ZUCCA

WWW.ICTSECURITYMAGAZINE.COM

INDICE

ABOUT THE AUTHOR 6

INTRODUZIONE 8

CAPITOLO 1 12

1.1 Dalla Scuola Ippocratica alla Digital Health 13

1.2 Definizione e aree tecnologiche di e-Health 15

1.3 La Telemedicina 17

1.4 Il Fascicolo sanitario elettronico 21

1.5 Nuovi scenari: la Telechirurgia 24

CAPITOLO 2 27

2.1 Un dato ad alta sensibilità 28

2.2 Principi cardine sulla protezione dei dati 32

2.2.1 Il principio di accountability 35

2.2.2 Il Data Protection Officer 37

2.2.3 Il registro delle attività di trattamento 39

2.3 Standard internazionali per la sicurezza dei dati: ISO 27001 40

2.4 Condizioni di liceità del trattamento in ambito sanitario 43

CAPITOLO 3 47

3.1 Rivoluzione digitale ed innovazione criminale 48

3.2 Alcune precisazioni terminologiche 52

3.3 Criminalità dipendente dalle nuove tecnologie 55

3.3.1 La triade CIA della sicurezza informatica 58

3.3.2 Sette principi di sicurezza 61

3.4 Nuovi autori: i cyber-criminali 64

3.5 Dagli hacker alle cyber-gang 67

3.6 Nuove vittime: le cyber-vittime 76

CAPITOLO 4 80

4.1 Report: un settore altamente vulnerabile 81

4.2 Nuova frontiera della privacy: la protezione dei dati personali 88

4.3 Nozione di Data Breach 93

4.3.1 Simulazione: una breccia in sanità 100

4.3.2 Il mercato nero della salute 106

4.3.3 Caso: Ulss 6 Euganea di Padova 112

4.4 Inquadramento giuridico: il reato informatico 116

4.4.1 L'accesso abusivo ad un sistema informatico o telematico 120

4.4.2 La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici 125

4.4.3 La diffusione di programmi diretti a danneggiare o interrompere un sistema informatico 127

4.5 Profili di interdisciplinarietà: il Codice Privacy 132

4.6 Le fasi di un attacco 136

4.7 Una rassegna di casi in sanità 143

4.7.1 WannaCry 144

4.7.2 Ospedale Universitario di Düsseldorf 146

4.7.3 Fatebenefratelli Sacco di Milano 148

4.8 Inquadramento giuridico: il danneggiamento informatico 150

4.9 Cybercrime as a Service: caso LockBit 156

4.10 La tecnologia al servizio della salute 162

4.11 Hacking medicale 167

4.11.1 Dispositivi IoMT a rischio: i casi 169

4.12 Sicurezza dei dispositivi medici: scenari regolatori 176

CAPITOLO 5 183

5.1 Il panorama normativo della cybersecurity 184

5.2 Linee guida ENISA 193

5.3 Readiness, response, recovery 199

5.4 Intervista: nell'ottica di un clinico 206

5.5 Intervista: nell'ottica di un ingegnere informatico 212

CAPITOLO 6 219

6.1 La matrice di rischio 220

6.2 Valutazione d'impatto (DPIA) 225

6.3 Capire, valutare e gestire il rischio cyber 231

6.4 Una visione d'insieme 236

CONCLUSIONI, NON CONCLUSIVE 242

RIFERIMENTI BIBLIOGRAFICI 248

ABOUT THE AUTHOR

Maria Vittoria Zucca

Dottoranda del Programma di Interesse Nazionale in Cybersecurity

Maria Vittoria Zucca, laureata con lode in Giurisprudenza presso l'università degli Studi di Trento, è attualmente dottoranda nel Programma di Dottorato di Interesse Nazionale in Cybersecurity, con istituzione capofila la Scuola IMT Alti Studi di Lucca, ed è affiliata alla Scuola Superiore Sant'Anna, presso l'Istituto Dirpolis (Diritto, Politica e Sviluppo). La sua attività di ricerca si concentra sulla prevenzione, l'indagine ed il contrasto della criminalità informatica, includendo le discipline del diritto penale dell'informatica e della criminologia digitale. Su questi temi è autrice di diverse pubblicazioni scientifiche e partecipa regolarmente a conferenze nazionali e internazionali.

INTRODUZIONE

Nel pieno dell'attuale Darwinismo digitale l'innovazione tecnologica non è più sentita quale requisito distintivo di aziende migliori o particolarmente capaci, ma anzi quale prerequisito imprescindibile, pena il diventare anelli deboli di una catena evolutiva in cui soltanto coloro che sono dotati di capacità d'adattamento possono sopravvivere. Fra gli svariati settori assoggettati a tale digitalizzazione rientra a piena regola quello sanitario, dove i sistemi informativi ne costituiscono ad oggi indispensabile ossatura.

È innegabile invero come la sanità sia stata sottoposta negli ultimi anni ad un inarrestabile processo di innovazione, ne sono un chiaro esempio l'evolversi della telemedicina, le cartelle cliniche elettroniche, la nanorobotica chirurgica, i dispositivi *wearables*, od altresì l'utilizzo delle intelligenze artificiali in ambito diagnostico. Sebbene i benefici sottesi a tale digitalizzazione siano d'immediata percezione in termini di maggiore celerità, organizzazione ed efficienza delle cure, parimenti evidenti risultano essere i rischi, le vulnerabilità e le minacce, derivanti sia da una ingente mole di dati ed informazioni in circolo, difficilmente controllabili, sia dall'utilizzo di sistemi, apparecchiature e *devices* spesso non congegnati seguendo elevati standard di sicurezza *by design*.

In particolar modo si sta attualmente assistendo all'emergere di innovative cyber-minacce, sempre più sofisticate, che privilegiano lo strumento cibernetico al fine di acquisire dati sanitari sensibili o per compromettere l'erogazione di un servizio essenziale dello Stato, pertanto la nuova "patologia" informatica che la sanità tutta si ritrova a dover fronteggiare risulta essere una rinnovata forma di criminalità informatica, contraddistinta dalle tipiche caratteristiche di impresa.

Si è ritenuto di condurre la qui presente trattazione servendosi del lessico medico, in particolar modo mutuandone l'iter operativo, per come costituito dalle fasi di anamnesi, diagnosi, passando per la terapia in atto, per giungere poi ad una prognosi del fenomeno oggetto di analisi.

Il quadro sintomatologico vede le infrastrutture critiche sanitarie del Paese, quali soggetti estremamente vulnerabili, contraddistinte sovente da arretratezza tecnologica e strutturale, dalla mancanza di risorse (sia umane che fisiche) e da una cybercultura inadeguata, nonostante siano al contempo bacini di un ingente pa-

trimonio informativo ultrasensibile, e parimenti garanti di funzioni cruciali della società, quali salute, sicurezza e benessere comuni. Sono le statistiche a parlar chiaro: la sanità risulta essere attualmente nel mirino di svariati attacchi hacker, le aggressioni digitali indirizzate a colpire tale settore sono in costante aumento, divenendo col tempo sempre più frequenti, gravi e pervasive.

Volendo diagnosticare le principali tipologie delle anzidette minacce cyber si è ritenuto opportuno tripartirle, in base al target di riferimento, nei sottogruppi: *data breach, ransomware* ed intrusioni nei dispositivi medicali.

La frase celebre di Lavoisier, recitante: *"nulla si crea, nulla si distrugge e tutto si trasforma"* sembra trovare smentita al sopraggiungere dell'informatica, una informazione può infatti ad oggi esser distrutta, alterata od altresì duplicata infinite volte, seguendo metodi tanto leciti quanto fraudolenti. Ed è così la sanità in primis dovrebbe risultare in grado di proteggere e vigilare su valori quali la riservatezza, l'integrità e la disponibilità circa la mole di dati ultrasensibili di cui è custode, quei medesimi dati che, in forma singola quanto aggregata, si figurano attualmente come ricco bacino di approvvigionamento per il cybercrimine, data la loro ampia versatilità ed il conseguente valore economico.

La minaccia principe comunque, per larga diffusione ed impatto, rimane il *ransomware,* quale *malware* rivolto a colpire le stesse infrastrutture, cifrandone i dati, danneggiando e causando la temporanea indisponibilità dei sistemi.

I settori critici, quale quello sanitario, rappresentano terreno fertile per tale tipologia di attacco, data la loro alta propensione a pagare ingenti riscatti al fine di difendere la propria *business continuity,* evitando le conseguenze economico sociali devastanti che potrebbero derivare da eventuali disservizi e rallentamenti operativi. Ancora, dato il pieno approdo nell'era *dell'Internet of Medical Things,* non sono da escludere tutta una serie di cyberminacce impattanti su dispositivi, strumenti ed apparecchiature medicali, ossia tanto sulla disponibilità del servizio che un dato *device* supporta, quanto sulla riservatezza dei dati da esso raccolti, nonché altresì sulla sicurezza del paziente stesso che ne stia facendo uso.

D'altronde se ad oggi i dispositivi medicali condividono gran parte della propria architettura con quella dei normali personal computer, ossia la presenza di un

sistema operativo, di una componentistica elettronica e di una interfaccia di comunicazione per connettersi con l'esterno, avranno parimenti in comune le stesse tipologie di minacce ed i conseguenti approcci di *security*.

Pertanto l'attuale terapia in atto, nonché conditio sine qua non della stessa innovazione tecnologica, risulta essere la cybersicurezza, intesa quale attività preventiva finalizzata a rafforzare la resilienza delle infrastrutture e la continuità dei servizi essenziali erogati. Di conseguenza l'attuale normativa tenderà ad incentivare l'adozione di una strategia olistica di "difesa in profondità", attuata mediante una metodologia di gestione del ciclo di vita della *cybersecurity*, che parta dall'analisi e dalla valutazione dei livelli di rischio, all'adozione di misure ed architetture di sistema atte alla mitigazione, gestione e *recovery* dai possibili incidenti, per giungere poi al continuo monitoraggio in tempo reale di sistemi e servizi sanitari, il tutto attraverso soluzioni sì intrinsecamente sicure e resilienti che, pur offrendo un alto livello di *security* e di *continuity*, non ostacolino mai la piena efficienza operativa dei sistemi medesimi.

In sede propriamente di prognosi non potrà che andarsi a delineare una sfida comune, rivolta a tutti quei soggetti appartenenti all'ecosistema sanitario, affinché siano informati, coinvolti, attivi e proattivi sul tema, riconoscendone la pressante urgenza e negando la marginalità che sovente in passato ha dovuto rivestire. Temi quali l'empowerment delle figure professionali in ambito cyber, la autonomia strategica, *l'awareness* e la responsabilizzazione saranno pertanto i traguardi a cui gli *stakeholders* della *cybersecurity* nazionale (istituzioni centrali o locali, nonché società civile) mireranno, attuando tutte quelle misure atte a far sì che il livello di resilienza possa incrementare e che i settori critici strategici necessari alla sussistenza dello Stato possano rivelarsi adeguatamente tutelati e protetti.

CAPITOLO 1

E-HEALTH: VERSO UNA SANITÀ DIGITALE

1.1 Dalla Scuola Ippocratica alla Digital Health

Si vuol dare avvio alla presente trattazione con un rapido *excursus* storico, senza alcuna pretesa di esaustività, sulle origini e sull'evoluzione della scienza medica, così da comprenderne il valore e l'intrinseca capacità di procedere di pari passo col progresso umano.

Una prima radicale svolta si registra nel V secolo a.C. con l'arrivo della medicina greca, la quale permise di abbandonare le precedenti pratiche rituali e divinatorie, tramutando la figura del medico da sciamano o sacerdote che fosse, a quella di un razionale pensatore, padrone di un sapere scientifico dedito all'osservazione, all'interpretazione dei fenomeni e alla ricerca delle loro cause.

Da qui Ippocrate, ritenuto il padre della medicina moderna, egli assegnava un compito puntuale alla medicina: *"Descrivere il passato, comprendere il presente e prevedere il futuro",* in pratica, agile viene il richiamo: l'anamnesi, la diagnosi, la prognosi della odierna medicina.[1] Una volta divenuto controllabile, disponibile alla discussione, nonché confutazione, il sapere medico, seguito dai primordiali studi anatomici e fisiologici, divenne oggetto di studio nelle prime scuole e, a seguire, nelle università.

Seguì poi per tutto il decorso storico un costante progredire della scienza medica parallelamente da una parte alle esigenze collettive: si sviluppò la pratica chirurgica a supporto delle campagne di guerra, si approfondirono gli studi sull'origine delle malattie epidemiche a seguito dell'arrivo in Europa della cosiddetta peste nera, e d'altra parte in parallelo all'evoluzione tecnologica: la diffusione del microscopio portò allo sviluppo dell'istologia, si svilupparono le prime tecniche radiologiche, vennero implementati gli esami fisico-chimici e biologici fino ad arrivare alle moderne sperimentazioni di laboratorio.[2]

---

1 R. Brischetto, F. Cosmi, *Imparare il metodo scientifico. Da Ippocrate a Garattini*, Edizioni LSWR, Milano, 2022.

2 Per una approfondita trattazione si rimanda a Jean-Charles Sournia, *Storia della Medicina,* Edizioni Dedalo S.r.l., Bari, 1994.

Si approda così al fenomeno che si erge a nucleo duro di questo lavoro tutto: l'avvento della rivoluzione digitale.

Non esiste settore della vita quotidiana (si pensi al settore bancario, finanziario, dei trasporti etc.) che non sia stato profondamente influenzato, modificato ed orientato dalle nuove tecnologie,[3] e l'ambito sanitario non si è mostrato di certo immune da tale digitalizzazione.

Si è assistito infatti ad un mutamento del paradigma della medicina tradizionale:[4] da una sanità basata su un sistema di comunicazione burocratico-cartaceo novecentesco, in cui le informazioni viaggiavano alla velocità di gambe e mani di assistenti ed impiegati, ad un sanità digitale, caratterizzata da istantaneità, celerità, nonché contraddistinta dalla de-materializzazione e dalle connessioni sociali.

Chiaro è come alle innovazioni tecnologiche si siano simultaneamente affiancati notevoli mutamenti sociali: l'invecchiamento della popolazione, la crescita delle aspettative di cura, la prevalenza delle patologie cronico-degenerative; tutti fattori che hanno contribuito a dare alla luce nuove domande indirizzate al sistema sanitario, in merito soprattutto alle modalità di erogazione delle prestazioni sanitarie stesse.[5]

Così ad oggi la piattaforma *Image-guided therapy,* lanciata da Philips, permette ad un medico di osservare a distanza un paziente valutando se una operazione sia necessaria o meno; oppure il progetto di intelligenza artificiale *"Watson"* della IBM è capace di processare in contemporanea una immensa mole di immagini (quali radiografie, risonanze, tomografie) e informazioni (dati medici, cartelle cliniche, sperimentazioni etc.) al fine di individuare velocemente specifici percorsi diagnostico-terapeutici; ed ancora il sevizio telematico di monitoraggio da remoto *Doctorplus*, destinato a pazienti affetti da diabete e scompenso cardiaco,

---

3 A. Antonilli, "Sicurezza informatica e trattamento dei dati in ambito sanitario", in *Salute e società,* XVI, suppl. 3/2017, p. 84 -100.

4 M. Moruzzi, "La nuova cultura della sanità dematerializzata", in *Recenti Progressi in Medicina*, vol. 105, n.11, 2014, p. 407- 409.

5 C. Cipolla, A. Ardissone, "Un paradigma cittadino-centrico nella m-Health", in *Salute e società,* XVI, n.2, 2017, p. 12-28.

permette di inviare via bluetooth le misurazioni fatte autonomamente dai pazienti ad una centralina, che a sua volta le inoltrerà ad una piattaforma cloud a cui avranno accesso il medico, lo specialista, ed altresì la centrale infermieristica. [6]

L'elenco sarebbe assai vasto: stampanti tridimensionali, dossier e fascicoli sanitari elettronici, dispositivi wireless, servizi di telesoccorso, terapie digitali, nanotecnologia e robotica chirurgica, tutto si trova ad essere inglobato nel capiente "termine ombrello" che prende il nome di *e-Health* (o sanità digitale).

1.2 Definizione e aree tecnologiche di e-Health

Il termine *e-Health* è divenuto popolare a partire dalla fine degli anni Novanta, coniato per essere in linea con le altre "parole elettroniche" quali e-commerce, e-business nel tentativo di trasmettere quello stesso entusiasmo che già ruotava attorno al commercio elettronico e per render conto delle nuove possibilità che Internet stava gradualmente aprendo al settore sanitario. [7]

Per cogliere il carattere multidisciplinare che si cela dietro a tale terminologia si voglia di seguito riportare la definizione offerta dal ricercatore tedesco-canadese Gunter Eysebanch: *"L'e-Health è un campo emergente dall'intersezione tra l'informatica medica, il sistema sanitario pubblico ed il mercato, che si riferisce ai servizi ed alle informazioni sanitarie forniti attraverso Internet e le tecnologie correlate. In senso più ampio, il termine caratterizza non solo uno sviluppo tecnico, ma anche una forma mentis, un'attitudine ed un impegno a pensare in senso globale, al fine di migliorare la sanità a livello locale, regionale e mondiale attraverso l'utilizzo di tecnologie dell'informazione e della comunicazione"*. [8]

Ancora, per maggiore chiarezza, può esser utile richiamare la definizione per come fornita dalla Commissione Europea, che così recita: *"L'e-Health risulta un*

---

6 *Ivi* p.15.

7 G. Eysebench, "What is e-Health", in *Journal of Medical Internet Research*, 3(2), 2001, p. 20.

8 *Ibidem.*

insieme di strumenti e servizi digitali al servizio della salute e delle cure mediche, implicanti l'uso di tecnologie informatiche e di telecomunicazione (ICTs) per migliorare attività come la prevenzione, la diagnosi e il trattamento delle patologie, nonché il monitoraggio e la gestione delle abitudini e stili di vita che incidono sulla salute".

È stato dunque il notevole sviluppo delle ICTs come pure il passaggio dal web 1.0 alla fase 2.0 ad aver ampliato il ventaglio dei servizi fruibili dai cittadini in ambito di salute, e benché l'e-Health sia un settore estremamente dinamico ed in costante evoluzione, si può qui tentare di elencarne le principali aree tecnologiche: la telemedicina (nelle sue forme di tele-diagnostica, tele-consulto, tele-assistenza, tele-chirurgia), le cartelle cliniche elettroniche, il telesoccorso, i dispositivi mobili indossabili e portabili, la robotica ed ancora la diagnostica avanzata assistita da algoritmi di intelligenza artificiale. [9]

L'esser catapultati nell'era *dell'Internet of Things* [10] ha permesso poi di coniare un sottoinsieme *dell'e-Health*: la *m-Health (o mobile health)* che vuole riferirsi a tutti i sensori, *mobile devices, apps, e wearable technologies* tramite cui l'utente interviene nella gestione della propria salute, potendo monitorare una vasta serie di parametri vitali (quali battito cardiaco, temperatura corporea, attività cerebrale, funzionamento metabolico etc.) dando così vita al fenomeno sociale del c.d. *self-tracking* consistente nel misurare, registrare e condividere quella grande mole di dati autoprodotti relativi al funzionamento del proprio organismo. [11]

Si vogliono concludere queste preliminari riflessioni evidenziando come i vantaggi offerti da una sanità digitale siano facilmente ed immediatamente percepibili: maggiore efficienza e qualità delle cure (si pensi all'accuratezza delle diagnosi o alla precisione delle procedure mediche etc.), riduzione dei costi economici,

---

9 Con l'espressione *"web 1.0"* si suole indicare un primordiale flusso comunicativo di tipo unidirezionale in cui viene fortemente limitata la possibilità di interazione tra una azienda ed i propri clienti, invece col passaggio allo stadio del *"web 2.0"* si approda ad una comunicazione di tipo partecipativo, contraddistinta dai tre pilastri di: interazione, condivisione e partecipazione.

10 *"Internet delle cose"* è una espressione coniata nel 2011 da Dave Evans, il quale ne parlava in questi termini *"L'internet delle cose indica semplicemente il momento in cui a Internet hanno incominciato ad esser più cose (o oggetti) che persone".*

11 C. Cipolla, A. Ardissone, op.cit. supra a nota 5, p.21.

maggiore partecipazione informata del paziente, prevenzione delle condizioni mediche gravi, riduzione del costo umano delle patologie ed anche un generale miglioramento del benessere personale.

Se i benefici sono senza dubbio evidenti tuttavia occorre volgere l'occhio anche agli elementi più di criticità: produrre e consumare contenuti elettronici implica la circolazione di una grande mole di dati ed informazioni, difficilmente controllabili e per questo potenzialmente esposti ad elevati livelli di rischio.[12]

È stato proprio l'irrompere dell'evoluzione tecnologica a far sorgere nuove problematiche di sicurezza, *rectius* cyber-sicurezza, e nello scenario sanitario tali preoccupazioni si sono materializzate col verificarsi di, sempre più frequenti, attacchi informatici (miranti ad esempio alla sottrazione di dati sensibili), tali da minare tanto la privacy quanto la dignità dei pazienti.

Si avrà comunque modo di analizzare compiutamente le questioni inerenti la cyber-sicurezza nonché il cyber-crimine in ambito sanitario più avanti nella trattazione, a cui si rimanda.

1.3 La Telemedicina

Risulta preliminare, per comprendere a pieno gli argomenti che in seguito verranno esaminati, chiarire cosa si debba intendere col termine di medicina a distanza (o telemedicina), anzitutto tramite qualche cenno storico.

È agli inizi del '900 che si fanno risalire i primi tentativi di quella che si può definire una telemedicina ante *litteram*: nel 1906 Willem Einthoven, uno dei padri dell'elettrocardiografia, fu il primo a studiare un elettrocardiogramma attraverso la linea telefonica, nel 1920, negli Stati Uniti, alcuni medici vennero ingaggiati per l'assistenza sanitaria via radio alle navi che avevano emergenze mediche, nel

12 A. Antonilli, op. cit. *supra* a nota 3, p. 88.

1955 l'Istituto Psichiatrico del Nebraska, tramite un collegamento che utilizzava la televisione a circuito chiuso, realizzò consulti fra specialisti per finalità didattiche nonché per effettuare terapie di gruppo, e ancora nel 1971 fu utilizzata, per la prima volta, la trasmissione satellitare. [13]

Indubbiamente però fu l'avvento di Internet a determinare una svolta rivoluzionaria: grazie alla rete infatti si è reso possibile registrare ed inviare enormi quantità di immagini, dati e audio consentendone l'accesso ad un numero praticamente illimitato di persone contemporaneamente, ed è così che la telemedicina ha potuto superare la propria fase di sperimentazione per radicarsi sempre di più nella quotidianità, modificando e migliorando il sistema socio-sanitario tutto.

Pertanto la telemedicina altro non è che un nuovo modo di concepire l'attività del medico, il quale grazie all'ausilio delle nuove tecnologie, riesce a controllare e monitorare i pazienti senza che questi ultimi siano fisicamente presenti: non è più il paziente a spostarsi, ma le informazioni che lo riguardano.

Seppur risulti difficile darne un'univoca definizione, essendo una disciplina in costante e dinamica evoluzione, si possono richiamare le parole di sintesi utilizzate nel 1997 dall'Organizzazione Mondiale della Sanità: *"La telemedicina è l'erogazione dell'assistenza sanitaria, quando la distanza è un fattore critico, da parte degli operatori sanitari; ed a tal fine sono utilizzate le tecnologie informatiche e le telecomunicazioni per lo scambio di informazioni per la diagnosi, la terapia, la prevenzione di patologie, per l'istruzione permanente degli operatori sanitari e per la ricerca e lo studio in tutti i settori di interesse per il miglioramento dello stato di salute dell'individuo e della comunità"*.

Si ricava dunque che la prestazione in telemedicina non sostituisce la prestazione sanitaria tradizionale, ma la integra per potenzialmente migliorarne efficacia, efficienza ed appropriatezza, pur conservando le implicazioni di un qualsiasi atto medico dal punto di vista professionale, etico, nonché legale.

---

13 E. Manzi, S. Selvaggi, V. Sica, "Tecnologie informatiche e delle comunicazioni in medicina: la telemedicina", in V. Sica, S. Selvaggi (a cura di), *La telemedicina. Approccio multidisciplinare alla gestione dei dati sanitari,* Springer-Verlag, Milano, 2010, pp. 1-9.

Per provvedere ivi ad una rapida classificazione, i servizi di telemedicina possono essere suddivisi in tre differenti macro-categorie: la telemedicina specialistica, la telesalute e la teleassistenza.[14]

Per quanto concerne la prima macro-categoria, a seconda del tipo di attori coinvolti (che siano medico-paziente od anche medico-altri operatori sanitari) la telemedicina specialistica segue tre distinte modalità:

a. La televisita: che consente al medico di vedere ed interagire a distanza col paziente, in tempo reale o differito, e ciò che scaturirà da tale rapporto sarà proprio un atto diagnostico contenente prescrizioni di farmaci o di terapie;

b. Il teleconsulto: un'attività di consulenza a distanza fra medici finalizzata ad ottenere pareri e consigli, in ragione di una specifica competenza medica, nella scelta di una terapia legata alla presa in carico di un paziente;

c. La telecooperazione sanitaria: ossia l'assistenza concreta fornita da un medico (od altro operatore sanitario) ad un altro medico impegnato in un determinato atto sanitario, ed è il termine utilizzato soprattutto per la consulenza fornita a quanti prestano un soccorso d'urgenza.

La seconda macro-categoria, quella della telesalute, comprende i sistemi che collegano i pazienti, in particolar modo coloro affetti da malattie croniche, con gli stessi medici affinché questi ultimi possano prestare loro assistenza a livello diagnostico, di monitoraggio, di gestione e di responsabilizzazione. Si rende necessario allora tanto un ruolo attivo del medico quanto del paziente che monitorerà e trasmetterà i propri dati (solitamente i parametri vitali di base) provvedendo alla propria autocura, autonomamente o con l'ausilio di un operatore sanitario.

---

14 *Linee di indirizzo nazionali sulla Telemedicina* approvate nella seduta del 10 Luglio 2012, dall'Assemblea generale del Consiglio Superiore di Sanità, reperibile al sito internet: https://www.salute.gov.it/portale/documentazione/p6_2_2_1.jsp?lingua=italiano&id=2129.

Infine la terza macro-categoria è quella della teleassistenza, un sistema socio-assistenziale per la presa in carico di una persona anziana o fragile, che vedrà la gestione di allarmi, l'attivazione di servizi di emergenza o chiamate di supporto, chiaro è come quest'ultima abbia contenuto prevalentemente sociale, con confini prettamente sfumati sul versante sanitario, con cui si dovrà in ogni caso connettere al fine di garantire una vera e propria continuità assistenziale.

Ancora una volta appaiono chiari e manifesti i benefici sottesi allo sviluppo e all'adozione di tecniche e strumenti di telemedicina, quali: l'equità di accesso all'assistenza sanitaria (si pensi alle aree rurali poco collegate alla città di riferimento, alle aree di montagna, alle piccole isole; od anche al miglioramento dell'assistenza sanitaria in carcere), una migliore qualità dell'assistenza atta a garantire continuità delle cure (si pensi al telemonitoraggio come strumento per migliorare la vita dei pazienti cronici attraverso soluzioni di auto-gestione), una migliore efficacia, efficienza ed appropriatezza delle cure prestate (si pensi al confronto multidisciplinare fra medici, all'ausilio per i servizi di emergenza-urgenza), la riduzione dei tempi di attesa e del ricorso alla ospedalizzazione, nonché la possibilità di ottimizzare l'uso delle risorse disponibili.

Altrettanto ovvia però appare l'esigenza di evitare un uso improprio della telemedicina: è indispensabile che i professionisti sanitari ed i pazienti siano adeguatamente formati e preparati a riguardo, così da garantire in primo luogo la sicurezza dei dati e di conseguenza la privacy degli individui.

Si può già anticipare in questa sede che il semplice utilizzo di ICTs per il trattamento di informazioni sanitarie o la condivisione online di tali dati non costituiscono di per sé strumenti di telemedicina, per esser più chiari: non rientrano nella telemedicina *social network, forum, newsgroup,* posta elettronica od altri canali non autorizzati.

A tal proposito si riportino a seguire le parole di Peter Zeggel, CEO di arztkonsultation.de, il principale fornitore di telemedicina in Germania: *"L'utilizzo di app che non sono progettate specificatamente per il settore sanitario comporta dei rischi. Le applicazioni di telemedicina sono progettate e certificate specificatamente per salvaguardare i dati personali sensibili. Bypassare questo alto livello*

di protezione significa rischiare di incorrere in una perdita di fiducia, nonché in misure disciplinari e sanzioni pesanti".

Da ultimo si sottolinei come ad oggi questo tipo di problematiche appaiano del tutto attuali: un report del 2021 commissionato da Kaspersky ad *Arlington Research,* condotto a livello globale e composto da 389 interviste fra coloro che operano nel campo della telemedicina ha dato alla luce tali risultati: il 54% dei fornitori di servizi di telemedicina concordano sul fatto che alcuni dei propri medici conducano abitualmente sessioni di medicina a distanza utilizzando app non specificamente progettate a tal fine quali FaceTime, Facebook Messenger, WhatsApp e Zoom. Inoltre sentimento diffuso fra gli operatori sanitari risulta essere proprio il timore di non riuscire a garantire la sicurezza e riservatezza dei dati sensibili: solo tre intervistati su dieci (30%) si dichiara infatti fiducioso che la propria azienda sanitaria sia in grado di intervenire efficacemente e bloccare eventuali intrusioni e violazioni informatiche.

Ciò inevitabilmente si riverbera anche sul versante dei pazienti: il 52% degli operatori sanitari ha sperimentato infatti casi di pazienti che si sono rifiutati di tenere videochiamate proprio per la diffidenza verso le tecnologie ed il timore in ambito di sicurezza e protezione dei dati. [15]

1.4 Il Fascicolo sanitario elettronico

Un referto scaturito da una sopraccitata prestazione di telemedicina e firmato digitalmente dal medico, dovrà poter essere condiviso, su richiesta del paziente, con altri sanitari in formato digitale, usando le più aggiornate soluzioni tecnologiche, fra cui il Fascicolo sanitario elettronico (d'ora in avanti indicato in breve come FSE). Decisive appaiono in materia nozioni quali la comunicabilità e l'interconnessione: le prestazioni sanitarie a distanza e il FSE possono e devono comu-

15 Kaspersky, *Telehealth take-up: the risks and opportunities,* healthcare report 2021.

nicare l'un l'altro in modo tale da innescare un flusso continuo di informazioni tali da consentire ai sanitari di poter sempre disporre di un quadro clinico corretto e il più esaustivo possibile rispetto i dati clinici di un paziente.

Il FSE è stato istituito con il decreto legge 179/2012, coordinato con la legge di conversione 221/2012, che si vuol qui richiamare a livello definitorio: *"Il fascicolo sanitario elettronico è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale"*. [16]

La normativa de quo prosegue poi delineandone in dettaglio le finalità : *"Il Fascicolo sanitario elettronico è istituito dalle regioni e province autonome [...] nel rispetto della normativa vigente in materia di protezione dei dati personali, a fini di: prevenzione, diagnosi, cura e riabilitazione; studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria"*. Si noti come delle tre finalità, soltanto la prima sia rivolta propriamente alla cura del cittadino, le rimanenti due riguardano invece la gestione della sanità pubblica, sia nella accezione di ricerca e sviluppo, sia per quanto riguarda la governance nazionale del sistema sanitario. [17]

Nel FSE confluiranno pertanto sia dati sanitari che amministrativi riferibili all'assistito, quali: dati identificativi del paziente; documenti sanitari e socio-sanitari (referti di laboratori, prescrizioni di medicinali, terapie, anamnesi, verbali di pronto soccorso etc.); il *Patient Summary* (anche "profilo sanitario sintetico") documento atto a riassumere la storia clinica del paziente e la sua situazione corrente, curato ed aggiornato dal medico di medicina generale; ed ancora vi sarà una autonoma sezione dedicata specificatamente al cittadino in cui inserire dati ed informazioni personali (dati sul nucleo famigliare, attività sportiva etc.). [18]

---

16 Legge 17 Dicembre 2012 n. 221, "Conversione in legge con modificazioni del decreto-legge 18 Ottobre 2012 n. 179, recante ulteriori misure urgenti per la crescita del Paese", entrata in vigore il 19 Dicembre 2012.

17 NETPATROL, "Sanità digitale e telemedicina: privacy, cybersicurezza e intelligenza artificiale nella sanità digitale", in GDPR *insight series,* n° 6, 2020, pp. 2-16

18 G. Ducci, "Pianificare la comunicazione dei servizi di e-health: attori, sistemi, relazioni. Il caso del fascicolo sanitario elettronico", in *Sociologia della comunicazione,* fascicolo 48, 2014, pp. 26-37.

Il sopraindicato decreto legge 179/2012 all'art 12, comma 3-bis prevedeva che il FSE potesse essere alimentato esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale avrebbe avuto quindi la facoltà di permettere o meno la costituzione del proprio FSE, come anche di decidere se e quali dati relativi alla propria salute inserire nel fascicolo medesimo.

Tale comma è stato tuttavia abrogato dal decreto legge 34/2020 recante "Misure urgenti in materia di salute e di sostegno al lavoro e all'economia" (c.d. decreto "Rilancio"), con simile abrogazione si è voluta facilitare l'alimentazione del FSE, in precedenza "limitata" dalla necessità del consenso, permettendo che in esso vadano a confluire direttamente i documenti sanitari appartenenti all'interessato (anche se generati da strutture sanitarie private o situate al di fuori della propria regione di appartenenza). [19]

Con tale mutamento allora si è voluta garantire una maggior completezza del FSE, ma di certo ciò non andrà ad incidere in alcun modo sul versante della privacy poiché l'accesso al FSE potrà comunque avvenire solamente previo consenso del soggetto interessato: sarà il cittadino invero a dover fornire l'autorizzazione affinché gli esercenti professioni sanitarie, sia pubblici che privati, possano accedere ai contenuti del FSE che lo riguardano, senza il suo consenso pertanto il FSE rimarrebbe comunque inaccessibile. A ciò fanno ovvia eccezione le Regioni ed il Ministero della Salute, che potranno trattare tali dati sanitari per finalità di governo e di ricerca, purchè in forma anonima e nel rispetto dei principi di indispensabilità, necessità, pertinenza e non eccedenza.

Ad ogni modo si specifichi ancora come la normativa privacy non sarà mai di intralcio alla tutela della salute: sia il decreto legge 179/2012, sia il GDPR prevedono infatti la possibilità di accedere al FSE nel caso in cui il paziente non sia nelle condizioni di prestare il suo consenso, ma l'accesso risulti comunque necessario per salvaguardare la propria vita o quella di terzi.

I brevi cenni che si sono fin qui voluti fornire miravano essenzialmente a presen-

---

19 Decreto legge 19 Maggio 2020, n. 34, "Misure urgenti in materia di salute, sostegno al lavoro ed all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19", convertito con modificazioni dalla legge 17 Luglio 2020, n.77.

tare il FSE quale il vero e proprio fulcro della *connected care* italiana, un nodo di aggregazione e condivisione di dati, documenti, analisi e statistiche.

Ciò tornerà senz'altro utile al prosieguo della trattazione dal momento che, come si vedrà, i dati sanitari protetti, quali informazioni altamente sensibili, non sono immuni da possibili interessi di mercato e possono pertanto rivelarsi ricco bacino di approvvigionamento per il cybercrimine.[20]

1.5 Nuovi scenari: la Telechirurgia

Dal nome dall'aviatore americano, Charles Lindbergh, che effettuò il primo volo senza scalo attraverso l'Oceano Atlantico, è passata alla storia come "Operazione Lindbergh", uno dei primi interventi chirurgici a distanza eseguito nel Settembre 2001 da un team di chirurghi con sede a New York su di un paziente ospedalizzato a Strasburgo.[21]

È dalla dimostrazione della fattibilità di tale procedura transatlantica che si sono poste le basi per la globalizzazione delle procedure chirurgiche: l'impiego della chirurgia robotica è ad oggi una realtà clinica invero pienamente inserita nella telemedicina, che va guadagnandosi sempre maggiori consensi.

Per telechirurgia in particolare si intende in una tecnica operatoria che consente al medico di eseguire un intervento chirurgico a distanza, ossia su di un paziente che non si trova fisicamente nello stesso luogo. L'operatore umano infatti si servirà di una apposita console, fornita di un monitor atto a consentire l'osservazione

---

20 Peraltro non si confonda il Fascicolo sanitario elettronico con il diverso strumento del Dossier sanitario elettronico (o DSE), la cui gestione viene affidata di norma ad un unico titolare del trattamento, con la finalità di rendere più efficienti i processi di diagnosi e di cura del paziente all'interno di un'unica struttura sanitaria, consentendo ai diversi professionisti che vi operano di accedere a tutte le informazioni cliniche relative a precedenti interventi (ricoveri, visite ambulatoriali etc.) purchè siano effettuati dall'assistito presso quella medesima struttura.

21 Marescaux, J. Leroy et al., "Transatlantic robot-assisted telesurgery", in *Nature*, vol. CDXIII, n. 6854, September 2001, pp. 379-380.

continua della regione operatoria, andando ad eseguire così tutte le varie manovre necessarie dell'intervento che, teletrasmesse, verranno con estrema precisione ripetute sul paziente da un robot chirurgico. [22]

La chirurgia a distanza allora, avvalendosi di reti wireless e tecnologie robotiche, potrebbe consentire la realizzazione di interventi chirurgici di alta qualità in luoghi con scarsa assistenza medica (si pensi ad aree rurali, o zone di guerra) eliminando la necessità di viaggi a lunga distanza; o permettere la collaborazione in tempo reale fra chirurghi situati in diversi centri medici; od ancora permettere di migliorare l'accuratezza chirurgica (ad esempio il tremore fisiologico dell'operatore può essere annullato). [23]

Si è pensato di inserire anche tale argomento in trattazione dal momento che il cyber-crimine in ambito sanitario non va ad esaurirsi nella mera violazione e sottrazione di dati ed informazioni sanitarie ultrasensibili, ma anzi la stessa *telesurgery* non si presenta immune da diversi aspetti critici legati proprio alla sua cyber-sicurezza.

A tal proposito, già in questa sede, si può riportare una sperimentazione portata avanti nel 2015 dalla ricercatrice Tamara Bonaci e dal suo team dell'Università di Washington, mirante ad analizzare le possibili minacce legate al settore della telechirurgia, in particolar modo guardando ai possibili attacchi informatici che possono andare ad interferire direttamente sul comportamento di un Telerobot. [24] Bonaci e i suoi collaboratori hanno in tale sede testato il robot per la telechirurgia denominato Raven II, analizzandone la capacità operativa sotto attacco informatico.

Il sopraddetto sistema Raven II risulta composto da due bracci chirurgici, controllati a distanza dall'operatore umano, progettato con l'obiettivo di lavorare con la

---

22 E. Santoro, V. Pansadoro, *La chirurgia robotica in Italia: indagine nazionale,* 2011.

23 Ovvio è che il chirurgo a sua volta riceverà informazioni dal campo operatorio, come immagini stereoscopiche tridimensionali e stimoli pressocettivi, che gli permetteranno di operare avendo l'illusione di essere in sala operatoria.

24 T. Bonaci, *To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robotics,* Department of Engineering, University of Washington, 2015.

massima efficienza in condizioni estreme, ed è proprio tale connotato a far sorgere una prima complicazione: i sistemi di *telesurgery*, dovendo operare in aree a rischio dispongono infatti di connessioni condivise, nonché di bassa qualità, con ovvie ripercussioni per quanto concerne privacy e sicurezza.

Nel condurre la sperimentazione il team di ricerca *de quo* è riuscito ad intromettersi nei comandi del robot, verificando la possibilità di prenderne il controllo, come anche di modificarne comandi ed operazioni effettuate nel corso dell'intervento chirurgico simulato.

Così spiega Bonaci: *"A causa della natura aperta e incontrollabile delle reti di comunicazione diventa facile per malintenzionati od hacker interrompere o interferire con la comunicazione tra un robot e un chirurgo"*.

Simulando un possibile attacco hacker pertanto i ricercatori sono stati quindi in grado di cancellare, riordinare e ritardare i comandi inviati tramite la console, di portare il telerobot ad uno stato di blocco ed altresì di prenderne il completo controllo.

Non può che essere allora una attuale preoccupazione quella di garantire requisiti minimi di sicurezza anche e soprattutto nell'ambito della telechirurgia, perché gravi ed irreversibili sarebbero le conseguenze di un reale *cyber attack* laddove vi sia concretamente la vita di un paziente sul tavolo operatorio.

CAPITOLO 2

IL TRATTAMENTO DEI DATI SANITARI

2.1 Un dato ad alta sensibilità

Così la Dr.ssa Salvadori Angelica, consigliere dell'Ordine dei Medici Chirurghi e Odontoiatri della Provincia di Torino: *"La prima cosa che faccio quando arrivo in studio è accendere il computer. E con questo gesto apro, in qualche modo inconsapevole, una finestra, anzi una porta attraverso la quale, nel corso della giornata, i dati dei miei pazienti potranno essere disseminati in molte direzioni. [...] Ad esempio, mi metto in collegamento con il SAR (Sistema di Accoglienza Regionale) della Regione Piemonte e il SAC (Sistema di Accoglienza Centrale) quando compilo in modalità informatica una ricetta dematerializzata contenente prescrizioni farmaceutiche e specialistiche, mi collego con AURA (Archivio Unico Regionale degli Assistiti della Regione Piemonte) se emerge l'esigenza di un aggiornamento dell'anagrafe degli assistiti, mi connetto con l'INPS (Istituto Nazionale della Previdenza Sociale) quando rilascio un certificato di malattia, oppure con l'INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) se devo certificare un infortunio lavorativo, con il CSI Piemonte (Consorzio per il Sistema Informativo) se devo vedere l'esito di un tampone per Covid 19, se devo richiederne uno, se devo verificare l'inizio o la fine di una quarantena o di un isolamento, se devo vedere se un paziente è vaccinato. E questo vale non solo per me, medico di medicina generale, ma per tutti i medici convenzionati con il SSN, per i medici specialisti ospedalieri e, per alcuni aspetti, anche per i medici liberi professionisti.*

Se i medici, forse, non sempre sono consapevoli di tutto quello che mettono in moto, viene da chiedersi: e i cittadini? Hanno una percezione corretta di tutte le strade che possono prendere i loro dati sanitari?". [25]

Nel discorrere del primo capitolo si è potuto constatare come, grazie alle potenzialità offerte dall'innovazione tecnologica, i dati sanitari stiano acquisendo sem-

---

25 A. Salvadori, "Deontologia e tutela dei dati sanitari", in *Torino Medica. La rivista dell'ordine dei medici chirurghi e odontoiatri della provincia di Torino*, anno XXXIII, numero 3-4, 2021, pp. 9-10.

pre maggior impiego nel mondo contemporaneo: dalla ricerca medica e farmaceutica alla gestione dei servizi sanitari pubblici e privati. [26]

La materia inerente alla protezione dei dati sanitari è stata definita "diritto inquieto" [27], vi è difatti una tensione che caratterizza i dati sanitari stessi: meritevoli da un lato di massima protezione e riservatezza, e dall'altro di una calibrata circolazione per esigenze di sanità pubblica (si pensi alla destinazione ai fini di ricerca). A tale poi già complesso bilanciamento si aggiunge il problema della sicurezza rispetto a possibili attacchi informatici che possono mettere a rischio tanto la privacy degli individui quanto la tutela della salute pubblica.

Occorrerà comunque dapprima inquadrare ontologicamente le categoria dei dati idonei a rivelare lo stato di salute.

Alquanto nota è difatti la formula che consente di qualificare i dati sanitari come "nocciolo (o nucleo) duro" della privacy, locuzione utilizzata da chi rileva come essi si collochino "nel cerchio concentrico più interno" o, se si vuole, all'estremo più elevato della "scala delle durezze" [28] della protezione dei dati personali, risultando invero capaci di far intravedere, quando non di svelare del tutto, la sfera più riservata della persona. [29] Ed è proprio dalla loro alta sensibilità che si ricava la necessità di una maggior tutela nel trattamento rispetto a quello indirizzato ad altre tipologie di dati, in quanto, se non correttamente svolto, potrebbe ingenerare rischi significativi per il rispetto dei diritti e delle libertà fondamentali dell'individuo, esponendo quest'ultimo a potenziali discriminazioni, stigmatizzazioni e classificazioni.

Il quadro normativo di riferimento è sicuramente esteso, ad ogni modo come

---

26 ANITEC-ASSINFORM (Associazione italiana per l'Information and Communication Technology), *Una data strategy per la Sanità italiana,* a cura del gruppo di lavoro Digital Transformation in Sanità di Anitec-Assinform, Maggio 2022, p. 20.

27 Intervento di A. Soro, ex-presidente dell'Autorità Garante per la protezione dei dati personali, "Tracciamento contagi coronavirus, ecco i criteri da seguire", in *Agenda Digitale,* 29 Marzo 2020.

28 L'immagine della scala delle durezze, diffusamente ripresa nella dottrina che si è occupata di privacy, si deve a Stefano Rodotà. Cfr. S. Rodotà, "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali", in *Rivista critica del diritto privato,* anno XV, 1997, pp. 583-609

29 F. Di Ciommo, "Il trattamento dei dati sanitari tra interessi individuali e collettivi", in R. Pardolesi (a cura di), *La privacy sanitaria,* vol. II, Giuffrè editore, Milano, 2003, vol. II, p. 239.

fonti principali si possono indicare il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio per come relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, anche meglio noto come GDPR *(General Data Protection Regulation)*, che abroga la direttiva 95/46/CE; [30] a cui si aggiunga il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, conosciuto anche come Codice della privacy), aggiornato ed integrato con le modifiche introdotte dal decreto legislativo del 10 agosto 2018, n. 101, quale recante disposizioni per l'adeguamento della normativa nazionale al regolamento (UE) anzidetto. [31]

Prima di affrontare la spinosa questione della protezione dei dati personali si vogliono fissare alcune preliminari definizioni, guardando innanzitutto alle disposizioni del Regolamento 2016/679/UE.

L'art. 4, par. 1, n. 1 del testo normativo sopraddetto infatti chiarisce come per dato personale si debba intendere: *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*.

Entro l'ampia categoria dei dati personali si rinviene poi il sottoinsieme dei cosiddetti "dati particolari" (ex dati sensibili, nel vecchio codice privacy), definiti dall'art. 9 del GDPR come: *"dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale,*

---

30 Regolamento (Ue) 2016/679 del Parlamento e del Consiglio, relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", del 27 Aprile 2016, che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), per il testo normativo nella sua completezza si rimanda al sito internet https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679.

31 Decreto legislativo 30 Giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal decreto legislativo 10 Agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (Ue) 2017/679 del Parlamento e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

Si noti come i dati relativi alla salute figurino proprio fra i dati particolari, cioè quei dati la cui conoscenza da parte di altri può recare un grave pregiudizio per l'interessato.

Addentrandosi ancora più nel dettaglio della normativa il Considerando 35 del GDPR puntualizza come fra i dati inerenti alla salute dovrebbero rientrare : *"tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. [...] Le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro"*.

Si comprende allora il motivo per cui i dati sanitari, ipersensibili, espressivi della più autentica essenza della privatezza, siano proprio quella tipologia di dati ad andare a beneficiare di una maggior tutela accordata dall'ordinamento, per come espressa in: misure di garanzia rafforzate, presupposti di liceità del trattamento particolarmente stringenti, stretta indispensabilità a fini informativi, divieto di divulgazione, e si intuirà altresì la ragione per cui siano necessitanti di una protezione rafforzata rispetto a tutti quei rischi di intrusione ed accesso indebito, alterazione e manipolazione connessi a possibili attacchi cibernetici indirizzabili ai sistemi informativi sanitari. [32]

---

32 Intervento di P. Stanzione, Presidente dell'Autorità garante per la protezione dei dati personali, "Sicurezza del dato sanitario e condivisione", in *Panorama*, 18 Febbraio 2022.

2.2 Principi cardine sulla protezione dei dati

Appurato come in ambito medico, ossia in qualsiasi struttura ospedaliera, RSA, ambulatorio del medico di base o del libero professionista, ad esser trattati sistematicamente siano soprattutto dati "particolari", si volgerà ivi lo sguardo alle disposizioni che vanno a disciplinarne le specifiche modalità di trattamento.

Preliminarmente tuttavia si passeranno in rassegna i sei principi generali, in tema di trattamento dei dati personali, elencati all'art. 5 del GDPR, quali presupposti fondamentali attorno a cui orbitano tutti i meccanismi di protezione dei dati.

In primis si annoveri il principio definito di liceità, correttezza e trasparenza *(lawfulness, fairness and transparency),* in nome del quale si richiede che i dati *"vengano trattati in modo lecito, corretto e trasparente nei confronti degli interessati",* ciò implica dunque che qualsiasi informazione ad essi inerente sia accessibile e di facile comprensione, grazie all'utilizzo di un linguaggio chiaro e semplice, nonché che gli interessati abbiano contezza dell'identità dei titolari del trattamento (ossia dei soggetti che per l'appunto trattano i dati personali) e delle finalità del trattamento stesso. Calando tale principio nel panorama sanitario si può richiamare quanto previsto dall'Accordo Stato-Regioni sulla telemedicina del 17 dicembre 2020, il quale prevede specifici oneri informativi nei confronti dei pazienti soggetti a servizi di telemedicina fra cui: una completa descrizione della gestione dei dati, dei diritti dell'assistito, delle modalità di contatto, nonché un elenco aggiornato dei responsabili del trattamento.[33]

Il secondo principio invece è relativo alla limitazione delle finalità *(purpose limitation)* dei dati, si rilevi come questi siano *"raccolti per finalità determinate, esplicite e legittime",* per cui non sarà consentito trattarli successivamente in modo non compatibile con le finalità previamente delineate. Si tenga comunque presen-

---

33 Il documento "Indicazioni nazionali per l'erogazione di prestazioni di telemedicina" è stato approvato dalla Cabina di regia del NSIS nella seduta del 28 ottobre 2020 ed è stato adottato con Accordo in Conferenza Stato Regioni del 17 dicembre 2020 (Repertorio atti n.215/CSR), si rimanda al sito https://www.statoregioni.it/it/conferenza-stato-regioni/sedute-2020/seduta-del-17122020/atti/repertorio-atto-n-215c-sr/.

te che eventuali ulteriori trattamenti per finalità di pubblico interesse, di ricerca scientifica, storica o a fini statistici non sono considerati incompatibili con le finalità iniziali e risultano pertanto consentiti.

Il terzo principio è la c.d. minimizzazione dei dati *(data minimisation)*, in ragione del quale questi ultimi dovranno essere *"adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati"*.

L'accuratezza poi *(accuracy)* è il quarto principio ed implica la necessità di garantire che i dati personali siano adeguatamente accurati ed aggiornati, ove necessario, adottando tutte le misure ragionevoli necessarie per cancellarli o rettificarli tempestivamente qualora inesatti rispetto alle finalità per cui vengono trattati.

Il quinto principio suole indicare la c.d. limitazione della conservazione *(storage limitation),* per cui i dati saranno *"conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati"*. Una eventuale conservazione per periodi di tempo più lunghi sarà consentita unicamente per finalità di interesse pubblico, di ricerca scientifica, storica o a fini statistici. Le politiche di data *retention*, previste specificatamente dal nostro ordinamento, disciplinano infatti numerosi e differenziati tempi di conservazione per quanto concerne la documentazione sanitaria: sarà pertanto compito dell'operatore sanitario (pubblico o privato) dover identificare la natura della documentazione e conseguentemente la normativa di riferimento applicabile. Per esemplificare, l'iconografia radiologica conta ad oggi un periodo di archiviazione di dieci anni, viceversa le cartelle cliniche, gli esami di laboratorio, i referti vedono un obbligo di conservazione illimitato nel tempo, in quanto rappresentanti atto ufficiale, indispensabile a garantire la certezza del diritto, nonché quale preziosa fonte documentaria per le ricerche di carattere storico sanitario. [34]

Il sesto ed ultimo principio riguarda infine l'integrità e la riservatezza dei dati *(integrity and confidentiality),* ciò implicherà che vengano adottate tutte le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza propor-

---

34 NETPATROL, op. cit. *supra* a nota 17, p. 8

zionato al rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, inclusa la protezione contro *"trattamenti non autorizzati o illeciti, la perdita, la distruzione o il danno accidentale"*.

A titolo esemplificativo, si richiami l'elencazione all'art 32 par.1 del GDPR relativamente alle misure che possono essere adottate ed implementate al fine di garantire la sicurezza dei *digital data,* fra cui:

a. La pseudonimizzazione dei dati personali, ovvero una metodologia che si pone l'obiettivo di "allontanare" il dato dalla persona, rendendone così complessa la stessa riferibilità (senza tuttavia romperne il legame, a cui mirano invece le tecniche di anonimizzazione);[35]

b. La cifratura dei dati, volta a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi tramite una apposita chiave di lettura idonea a decriptarne l'informazione;

c. La capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità ed altresì la resilienza dei sistemi e dei servizi di trattamento;

d. La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

e. L'auditing, espressione volta ad indicare una procedura atta a testare, verificare, e valutare regolarmente l'efficacia delle misure tecniche e organizzative concretamente adottate.[36]

Si badi bene, il legislatore non entra nel dettaglio, anzi quello fornito risulta pressoché un elenco generale, poiché è fondamentale che la *security* stessa venga garantita da soluzioni ritagliate nel modo più personale possibile rispetto alle

---

35 G. D'Acquisto, M. Naldi, Big Data e Privacy by Design. *Anonimizzazione, Pseudonimizzazione e Sicurezza,* Giappichelli Editore, Torino, 2017.

36 A. Antonilli, op. cit. *supra* a nota 3, p. 92

specificità del soggetto da proteggere. Non pare essere dunque "codardia legislativa", ma diretta conseguenza dell'assunto secondo cui se il titolare del trattamento deve essere accountable allora dovrà parimenti essere libero di ritagliarsi il "vestito" di sicurezza che ritiene necessario per la propria struttura.

2.2.1 Il principio di accountability

Il medesimo art. 5 del GDPR, al secondo paragrafo, enuncia il principio di responsabilizzazione (o *accountability*), in assenza del quale i sei principi cardine previamente elencati non potrebbero esser attuati: sarà infatti precipua responsabilità del titolare del trattamento [37] predisporre e mettere in atto specifiche soluzioni tecniche e organizzative che rendano il trattamento lecito, corretto, trasparente, adeguato, limitato nel tempo, pertinente ed effettuato per finalità legittime; così come sarà sua stessa responsabilità risponderne e "render conto" dell'efficacia delle misure concretamente impiegate e dei risultati così ottenuti.

Pertanto la figura apicale di una data struttura (si pensi ad un Direttore sanitario), tenuto conto della natura del dato, del suo ambito di applicazione (nell'erogazione di servizi di cura, in un progetto di ricerca etc.), del contesto (limitatamente alla propria struttura, od in condivisione con altre), delle finalità del trattamento, dei rischi per i diritti e le libertà delle persone fisiche, dovrà adottare misure tecniche ed organizzative adeguate, ossia parametrate al livello di rischio rilevato. Le anzidette misure poi, ex art. 24 GDPR, dovranno essere *"riesaminate ed aggiornate qualora necessario"*, introducendo così il principio fondamentale della ciclicità della sicurezza, quale perimetro altamente dinamico da dover revisionare periodicamente nel tempo, al fine di ottenerne un sempre maggiore perfezionamento. [38]

---

37 Per "titolare del trattamento" si rimandi all'art 4 del GDPR: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali […]"*

38 P. Perri (intervento), durante il Webinar "Conoscere e prevenire gli attacchi cyber in sanità", tenutosi in data 30 giugno 2021.

Non vi è dubbio sul fatto che venga in tal modo a delinearsi un sistema di adeguamento al GDPR fortemente accentrato sulla figura del titolare del trattamento: data la riconosciuta difficoltà di esercizio dei diritti dell'interessato,[39] essendo egli spesso propenso a rilasciare i propri dati con leggerezza o con carenza di consapevolezza, viene spostato il baricentro della responsabilità sul titolare del trattamento e sulla necessità che le operazioni di trattamento stesse siano *"GDPR compliant"*.[40]

Ed è proprio così che il concetto di *accountability* si collega con quelli di prevenzione e proattività, inglobando il saper agire d'anticipo, pianificando, mediante policy e tecnologie efficaci, quanto necessario per evitare i rischi di compromissione dei dati. Fare ciò significa, ex art. 25 GDPR, operare una valutazione del rischio e del suo contenimento attraverso tecniche di protezione "fin dall'avvio del trattamento" *(c.d. privacy by default)* e "per impostazione predefinita" *(c.d. privacy by design):* tali espressioni puntualizzano come la privacy degli interessati dovrà essere tutelata fin dall'inizio, cioè dalle fasi di ideazione e progettazione del servizio, e che non potranno esser trattati dati personali ulteriori rispetto a quelli minimi indispensabili per la specifica finalità del trattamento.[41]

Tali ragionamenti, per ciò che ivi più interessa, possono certo essere calati in ambito sanitario: i software, i dispositivi e le procedure utilizzati nella sanità digitale dovranno essere rispettosi della normativa in tema di protezione dei dati. Pertanto una corrispondenza di telemedicina fra medico e paziente con l'uso di sistemi non sicuri, come i social o la posta elettronica, costituisce di per sé una procedura a rischio, violante le regole sulla protezione dei dati, ed in quanto tale sanzionabile dall'Autorità Garante per la protezione dei dati.

Allora i sanitari, e le strutture che offrono servizi di telemedicina, hanno il precipuo dovere di gestire i rischi derivanti dal trattamento dei dati personali dei pa-

---

39 Per "interessato" si intenda la persona fisica alla quale si riferisce il dato personale.

40 D. Poletti, "Comprendere il Reg. UE 2016/679: Un'introduzione", in A. Mantelero, D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna,* Pisa University Press, 2018, pp. 9-19.

41 A. Cortesi, "L'art. 25 del GDPR: dalla privacy by default al principio di minimizzazione o necessità nel trattamento dei dati personali", in *Interlex: rivista di diritto, tecnologia, informazione,* pubblicazione iscritta nel registro della stampa del Tribunale di Roma con il n. 585/97, 2017.

zienti, optando per quelle soluzioni operative che offrano le migliori garanzie di proporzionalità, efficacia, sicurezza, e rispetto dei diritti della persona. [42]

Si voglia, già in questa sede, anticipare l'assoluto rilievo dell'innestare una cultura della (cyber)sicurezza mediante una adeguata formazione del personale medico, ed è così invero che recita l'articolo 32 comma 4 del GDPR: *"Il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare medesimo."* Si pensi ad una struttura sanitaria complessa (da un poliambulatorio ad un grande ospedale), in questa stessa gli operatori a trattare dati sanitari sono indubbiamente molteplici, ad ogni modo comunque tutti dovranno essere a conoscenza circa le procedure da seguire ed i conseguenti probabili rischi insiti nel trattamento di dati sensibili, in particolar modo alla luce delle sempre più frequenti compromissioni degli archivi e sistemi digitali sanitari.

2.2.2 Il Data Protection Officer

Anche la designazione di un Responsabile della protezione dati (da qui in avanti indicato come DPO, acronimo inglese per *Data Protection Officer*) rientra nell'approccio responsabilizzante delineato dal GDPR, in linea col principio di *accountability*.

Tale figura professionale, designata dal titolare o dal responsabile [43] del trattamento, si presenta quale un consulente esperto, dotato di un'approfondita conoscenza della normativa e delle prassi in tema di gestione dei dati personali, nonché dello specifico settore di riferimento in cui si trova ad operare.

La nomina del DPO si presenta come obbligatoria, ex art. 37 del GDPR, ogniqualvolta il trattamento sia effettuato da una autorità pubblica o da un organismo

---

42 NETPATROL, op. cit. *supra* a nota 17, p. 9.

43 Per "responsabile del trattamento" si rimanda all'art. 4 del GDPR: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento."*

pubblico, nonché quando le attività principali del titolare o del responsabile del trattamento consistano nel trattare, su larga scala, categorie particolari di dati personali (quali per l'appunto sono i dati inerenti alla salute).

Questo non significa che ogni medico sia obbligato a designare un DPO: il singolo professionista o il medico di base non trattano dati "su vasta scala", diversamente il problema si pone per gli studi in cui operano più medici e così anche per una Azienda sanitaria, un ospedale privato, una residenza sanitaria assistenziale, tutti si doteranno di tale figura dotata di competenze giuridiche, informatiche, nonché di *risk management,* la cui responsabilità sarà quella di osservare, valutare ed organizzare la gestione del trattamento dei dati personali (e dunque la loro protezione), affinché questi ultimi siano trattati nel rispetto delle normative privacy europee e nazionali.

L'art. 39 del GDPR opera poi una dettagliata elencazione delle principali funzioni del DPO, fra cui:

a. Informare e fornire una consulenza al titolare o al responsabile del trattamento in merito agli obblighi derivanti del Regolamento europeo;

b. Sorvegliare l'attuazione del Regolamento europeo, come anche vigilare sull'applicazione delle politiche del titolare del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti;

c. Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne il concreto svolgimento. Essendo la valutazione d'impatto un processo volto a valutare la necessità e proporzionalità di un determinato trattamento e a gestirne gli eventuali rischi, il titolare del trattamento si consulterà preventivamente col DPO su tematiche quali: condurre o meno la valutazione stessa, quale specifica metodologia sia da adottare, quali salvaguardie e misure di sicurezza siano

da applicare al fine di attenuare i rischi per i diritti delle persone interessate;

d. Fungere da punto di contatto per il Garante per la protezione dei dati personali e controllare che sia dato seguito alle richieste del Garante stesso.

Ancora, al secondo paragrafo l'art. 39 del GDPR con una formula prettamente di chiusura: *"Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo"*, in sostanza con tale disposizione di portata generale si chiede al DPO di delineare un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. [44]

2.2.3 Il registro delle attività di trattamento

Rientrante a sua volta nel concetto di *accountability* risulta essere anche il cosiddetto Registro delle attività di trattamento, novità introdotta dall'art. 30 del GDPR.

Quest'ultimo altro non è che lo strumento attraverso il quale il titolare e il responsabile del trattamento documentano in forma scritta, anche elettronica, le principali informazioni relative alle attività di trattamento e alle misure di garanzia adottate, in base alle finalità perseguite ed ai profili di rischio rilevati, al fine di poter poi dimostrare all'Autorità di controllo (il Garante per la protezione dei dati) di aver adempiuto correttamente alla propria funzione di protezione dei dati personali.

Per quanto concerne propriamente l'ambito sanitario la regolare tenuta del Registro delle attività di trattamento risulta quale obbligo per tutti gli operatori sa-

---

44 "Linee guida sui responsabili della protezione dei dati", WP243 rev. 01, adottate dal Gruppo di lavoro articolo 29 in materia di protezione dei dati personali, versione emendata ed adottata il 5 aprile 2017.

nitari (singoli professionisti sanitari, medici di medicina generale, ospedali privati, case di cura, farmacie, parafarmacie, Aziende Sanitarie appartenenti al S.S.N. etc.).

Per analizzarne nel dettaglio il contenuto minimo si guardi alla elencazione fornita all'art. 30 del Regolamento, in base al quale il Registro conterrà:

a. Il nome e i dati di contatto del titolare del trattamento;

b. Le finalità del trattamento (come "trattamento dei dati del paziente per l'erogazione della specifica prestazione sanitaria");

c. Una descrizione delle categorie di interessati (ad esempio "pazienti") e circa le categorie di dati personali (quali dati anagrafici, dati biometrici etc.);

d. Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati (si pensi ad un laboratorio analisi);

e. Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

f. Ove possibile, una descrizione generale circa le misure di sicurezza tecniche ed organizzative adottate (quali *security policy,* sistemi di *intrusion detection* etc.).

Potrà ad ogni modo esser riportata nel registro qualsiasi informazione che il titolare od il responsabile ritengano utile dover indicare (come le valutazioni di impatto effettuate o le modalità di raccolta del consenso seguite).

2.3 Standard internazionali per la sicurezza dei dati: ISO 27001

Come si è potuto osservare poc'anzi la normativa europea pone in capo ai titolari e responsabili del trattamento dei dati numerosi adempimenti, fra i quali assume notevole rilievo l'adozione di *"misure tecniche e organizzative adeguate per*

garantire un livello di sicurezza adeguato al rischio". Così infatti dispone l'art. 32 del GDPR cercando di guidare la scelta di tale misure in base al principio di adeguatezza, nonché *"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 ed anche le libertà delle persone fisiche"*. Essendo tali ultime formule pressoché generali, l'esigenza attuale risulta quella di fornire ai titolari e ai responsabili del trattamento degli strumenti concreti per individuare e scegliere idonee misure di sicurezza ed essere in grado di dimostrane la pratica adozione. [45]

Nel classificare invero le misure di sicurezza adottabili il GDPR opera un riferimento a due categorie di misure: quelle tecniche e quelle organizzative, diversamente dalla letteratura del settore [46] che invece distingue in: misure volte a garantire la sicurezza organizzativa (quali procedure di gestione di *data breaches*), quelle relative alla sicurezza logica e tecnologica (quali sistemi di autenticazione, *antimalware, firewall,* monitoraggi, scansioni delle vulnerabilità), e quelle relative alla sicurezza fisica (si pensi alla sicurezza degli edifici e degli archivi, al controllo degli accessi ed alla sicurezza ambientale). L'obiettivo di tutte le anzidette misure sarà comunque quello di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi informativi.

Con l'obiettivo di agevolare la specifica scelta delle misure di sicurezza concretamente adottabili da parte del titolare e del responsabile del trattamento soccorrono sul piano internazionale le c.d. normative ISO, ossia norme tecniche sviluppate dalla International *Organization for Standardization* riportanti linee guida che un determinato soggetto dovrà andare a rispettare per l'ottenimento di una certificazione valida sul piano internazionale, attestante la conformità del soggetto stesso (persona fisica, ente pubblico o privato) a specifici parametri di valutazione.

Fra la molteplici norme ISO, si può qui porre in evidenza la ISO 27001 quale standard internazionale per la sicurezza delle informazioni, creata al fine di definire i

---

45 R. Riccio, "Le misure di sicurezza tra GDPR e ISO 27001: due normative a confronto e i possibili scenari prospettabili", in *Cyberlaws: free legal database and blog,* 9 Gennaio 2019.

46 G. Butti, A. Piamonte, *GDPR: nuova privacy. La conformità su misura, Iter editore, Milano, 2017.*

requisiti atti a stabilire, implementare, mantenere e migliorare un sistema di gestione della sicurezza delle informazioni. [47]

Nei suoi contenuti presenta infatti un insieme di *best practices,* utili per sviluppare ed accrescere la capacità delle organizzazioni di gestire i rischi legati alla protezione dei dati, la ISO 27001 è invero molto specifica nel raccogliere, nel suo cosiddetto *annex* A, un vero e proprio catalogo di misure da adottare per contrastare nonché mitigare i rischi di perdita, modifica, divulgazione non autorizzata od accesso ai dati personali trattati.

Non sarebbe del tutto errato pensare quindi alla normativa GDPR e alla ISO 27001 alla stregua di un sistema integrato in ambito di sicurezza dei dati, d'altronde è lo stesso *Considerando* 100 del GDPR ad incoraggiare *"l'istituzione di meccanismi di certificazione"* che possano consentire di valutare il livello di protezione dei dati prodotti e dei servizi.

Ed ancora, è l'art. 24, comma 3 del GDPR a specificare come l'adesione ai codici di condotta ed alle certificazioni approvate, proprio come la ISO 27001, possa essere considerata come un elemento dimostrativo circa la conformità ed il rispetto degli obblighi del titolare del trattamento, in ossequio allo stesso principio di *accountability*.

Purtuttavia pare ovvio sottolineare come la garanzia di una certificazione non reciderà mai del tutto il rischio di verificazione di eventi dannosi relativi alla sicurezza dei dati, come peraltro si constaterà a seguire in ambito sanitario, ma al massimo andrà ad attenuarne le possibilità ed eventualità di accadimento e, conseguentemente, le relative responsabilità per tutti coloro che trattano i dati e le informazioni.

---

47 ISO/IESC 27001: 2013, "Information technology - Security techniques – Information Security - Managements systems – Requirements".

2.4 Condizioni di liceità del trattamento in ambito sanitario

Rimane tuttora da chiarire cosa si debba intendere con la precisa locuzione "trattamento dei dati", di qui la definizione fornita dall'art. 4 del GDPR: *"Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, ed altresì la cancellazione o la distruzione".*

Si può evidenziare peraltro come una operazione di trattamento si articoli in differenti fasi: una preliminare (raccolta e registrazione), una di elaborazione (selezione, impiego), una di circolazione (o diffusione), ed infine una residuale (conservazione, cancellazione).

Si vuole sottolineare come l'art. 9 del GDPR ponga un divieto generale al trattamento di intere categorie particolari di dati, fra cui figurano proprio i dati relativi alla salute: *"È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".*

Tuttavia tale divieto non è certo assoluto, in quanto in presenza di tutta una serie di condizioni di liceità, espressamente elencate dallo stesso testo normativo, tale preclusione non opera.

Per ciò che ivi interessa, il trattamento dei dati sanitari sarà considerato lecito laddove avvenga: per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale (cosiddetta "finalità di cura"); per motivi di interesse pubblico nel settore della sanità pubblica (si pensi alla gestione di emergenze sanitarie nazionali, od alla protezione da gravi minacce per la salute a carattere transfronta-

liero); ed ancora a fini di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici.

Vale la pena soffermarsi su come di fatto il GDPR superi così la precedente cornice normativa "consensocentrica" (propria del d.lgs. 196/2003, Codice privacy): diversamente dal passato infatti, non dovrà più esser richiesto il consenso del paziente per il trattamento di dati in ambito sanitario, purché si tratti di dati specificatamente necessari alle "finalità di cura" previste dal Regolamento Ue (prevenzione, diagnosi etc.) e che le relative attività siano effettuate da un professionista sanitario soggetto al segreto professionale.

Così, per esemplificare, persegue una finalità di cura l'infermiere che effettua una valutazione dei parametri vitali di un paziente al momento dell'accesso in pronto soccorso, come anche il cardiologo che raccoglie l'anamnesi necessaria alla corretta refertazione di un elettrocardiogramma; lo specialista che annota i dati biometrici del paziente in vista di un intervento chirurgico, come pure, in senso ampio, un direttore sanitario di una struttura pubblica che procede alla archiviazione di dati per studi statistici finalizzati tutela della salute collettiva. [48]

Ovvio è, ma vale la pena specificarlo, che non si deve qui confondere il consenso prestato al trattamento dei dati sanitari, col consenso ai trattamenti sanitari stessi: è quest'ultimo infatti a costituire il presupposto di legittimità dell'operato medico, andando ad "assorbire" il primo consenso, che non risulta più pertanto necessario.

D'altronde un professionista sanitario dovrà necessariamente venire a conoscenza di tutta una serie di dati identificativi e clinici (anamnesi, farmaci assunti etc.) per l'esecuzione di un trattamento sanitario, ed egli stesso, d'altra parte, nel trattare il paziente andrà a generare tutta un'altra serie di dati (referti, lastre etc.), dal momento poi che la semplice raccolta e consultazione di dati ne costituisce per definizione un trattamento, per un medico risulterà inevitabile, nello svolgimento delle sue funzioni, trattare costantemente i dati personali dei pazienti.

---

48 G. Chiarini, "Privacy: come cambia il dato normativo", in *E-Health: innovazione e tecnologia in ospedale,* vol. 72, 2019, p. 66-69.

Si segnali ancora come ai trattamenti “per finalità di cura” siano comunque equiparati anche i trattamenti operati tramite applicazioni mediche, quando la finalità perseguita è quella di fornire cura al paziente, tramite un servizio di telemedicina, telesorveglianza o telemonitoraggio.

È evidente inoltre come tale dispensa dall’ottenimento del consenso non opererà laddove i trattamenti dei dati dei pazienti avvengano per finalità diverse da quelle strettamente di cura (si pensi a fini promozionali, commerciali o di fidelizzazione della clientela).

Residuano ad ogni modo alcuni casi in cui i dati sanitari possono essere trattati esclusivamente con il consenso della persona interessata quali: come si diceva nel primo capitolo, la possibilità di accesso al FSE (fascicolo sanitario elettronico), l’adesione a servizi di refertazione online, oppure l’utilizzo di apps mediche, quando il trattare i dati del paziente afferisce, solo in senso lato, alla cura di quest’ultimo, ma non è ad essa strettamente necessario (si pensi ad una applicazione che fornisce indicazioni su come migliorare la qualità del sonno), in tal caso il titolare del trattamento dovrà trattare i dati previa acquisizione del consenso dell’utente interessato.

Si può concludere evidenziando come l’approvazione del GDPR abbia indubbiamente contribuito a richiamare l’attenzione degli operatori sanitari sui temi della privacy e della protezione dei dati, in quanto strettamente connessi ai profili della sicurezza delle cure e di dignità del paziente. Come evidenziato infatti dal Garante, nella sua relazione annuale al Parlamento dell’anno 2018, [49] eventuali carenze in ambito di sicurezza dei dati personali possono avere effetti oltremodo deleteri negli stessi processi di erogazione dei trattamenti medici, rappresentando causa di disfunzioni, rallentamenti ed errori sanitari, fonti di potenziale responsabilità della struttura sanitaria, obbligata così a risarcirne i danni conseguenti.

L’obbiettivo di questi due preliminari capitoli voleva essere il presentare la digitalizzazione della sanità quale occasione senza precedenti di sviluppo ed innovazio-

---

49 La Relazione del Garante per la protezione dei dati sanitari al Parlamento del 2018 è reperibile al sito internet: https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2018.pdf/e5bc382b-c5e9-b41b-b0d8-882f0904e546?version=1.0

ne, da dover senza dubbio promuovere per una sempre maggiore efficienza ed universalità delle cure, e per una migliore programmazione della spesa sanitaria. Tuttavia suddetta *digital health* dovrà realizzarsi all'interno di un progetto di politiche pubbliche organico e lungimirante di governance sanitaria, che promuova una condivisione selettiva dei dati sanitari, con le dovute cautele, al fine di minimizzarne i rischi cibernetici e le conseguenti possibili lesioni alla sfera personale della riservatezza e della dignità dei pazienti. [50]

50 P. Stanzione, intervento cit. *supra*, a nota 32.

CAPITOLO 3

IL NUOVO VOLTO DELLA CRIMINALITÀ

3.1 Rivoluzione digitale ed innovazione criminale

"Il settore della sanità è tra i più bersagliati al mondo per la quantità e la qualità di dati sensibili che custodisce e che ovviamente hanno un grande valore economico" così asserisce Alessandro Fontana, head of sales di Trend Micro Italia, azienda altamente specializzata in cybersecurity.

Sullo stesso tema approfondisce poi Sofia Scozzari, membro del comitato scientifico di Clusit (Associazione Italiana per la Sicurezza Informatica): *"Nel 2021, su un campione di 2.049 gravi attacchi individuati a livello globale, le aggressioni digitali verso questo settore sono state 262 (un dato in crescita del 24.8% rispetto al 2020), rappresentanti il 13% degli attacchi totali (erano il 10% nel 2018 e l'11% nel 2019 e 2020).* [51] *[...] Cresce soprattutto la gravità degli attacchi e questo è l'elemento più preoccupante, indice del fatto che i criminali sono decisi a causare più danni possibile verso un settore di importanza cruciale per la popolazione, in modo da esser certi di massimizzare i profitti".* [52] Si tenga a mente come il rapporto Clusit basi le proprie valutazioni unicamente su di un campione di cyberattacchi di notevole gravità (che hanno avuto cioè significativi impatti in termini di perdite economiche o di diffusione di dati sensibili) e di pubblico dominio, rappresentanti quindi una sottostima, o la proverbiale "punta dell'iceberg" del numero effettivo di *cyber attacks* sferrati quotidianamente che vengono bloccati o di cui non si viene a conoscenza.

Prima di volgere l'attenzione ad una approfondita analisi circa le tipologie di cyber-condotte criminose minanti *l'healthcare system*, occorre brevemente soffermarsi su che cosa si debba intendere parlando di cybercriminalità.

È in questi termini invero che lo scrittore William Gibson nel suo romanzo Neuromancer ipotizzava l'esistenza di un realtà sociale, uno spazio virtua-

---

51 R. Corcella, "Attacchi informatici in aumento nel settore sanitario", in *Corriere Salute,* Raffaello Cortina Editore, 10 Marzo 2022, p. 16

52 Per una approfondita panoramica degli eventi di cybercrime avvenuti a livello globale nel 2021, confrontandoli con i dati raccolti negli anni precedenti, si rimanda al *Rapporto Clusit sulla sicurezza ICT in Italia,* edizione Marzo 2022 reperibile al sito internet https://clusit.it/rapporto-clusit/

le quasi indipendente dalla realtà fisica, denominato per la prima volta col nome di cyberspazio: *"Una rappresentazione grafica di dati estratti dai registri di ogni computer del sistema umano. Complessità impensabile. Fasci di luce si estendono nel non-spazio della mente, ammassi e costellazioni di dati"*. [53]

Ad oggi gli scenari descritti da Gibson non sembrano più appartenere alla sola dimensione del romanzo di fantascienza, ma anzi sono divenuti centrali nelle riflessioni riguardanti la configurazione assunta dalla nostra società, una società a tutti gli effetti digitale. [54]

La fine del ventesimo secolo è difatti stata descritta come l'era di una nuova rivoluzione [55] legata principalmente alla diffusione della Rete Internet, congeniata negli anni Sessanta da parte del Ministero della Difesa Statunitense come progetto di importanza strategica, per poi andarsi progressivamente ad allontanare dalle primordiali finalità militari, imponendosi come strumento di *mass-communication* diffuso su scala planetaria.

Se gli strumenti digitali, il cyberspazio, e le forme sociocomunicative ad essi legate sono associati a decisivi cambiamenti in tutti gli aspetti della vita sociale quotidiana, questi stessi effetti possono essere osservati anche per quanto riguarda l'agire criminale. [56]

Pertanto le innovazioni culturali e scientifiche, indotte da tale rivoluzione digitale, si sono imposte parallelamente all'incremento di una *new crime's way* particolarmente complessa: [57] d'altronde dove esistono nuovi fatti sociali, nuove abitudini, nuove modalità per incontrarsi, pagare, proteggere i propri beni, nuove identità

---

53 W. Gibson, *Neuromante,* Mondadori, Milano, 2003.

54 G. Macilotti , "La criminalità informatica e telematica fra antichi dilemmi e nuove sfide", in A. Balloni, R. Bisi, R. Sette (a cura di), *Principi di criminologia applicata. Criminalità, controllo, sicurezza,* Wolters Kluwer-Cedam, Milano, pp. 251-277.

55 M. Castells, *La nascita della società in rete,* Egea, Milano, 2022.

56 G. Macilotti, "Studiare la cybercriminalità: alcune riflessioni metodologiche", in *Rivista di criminologia, vittimologia e sicurezza,* Vol. XII, N. 1, 2018, pp. 52-80.

57 G. Marotta, *Tecnologie dell'informazione e comportamenti devianti,* Edizioni Universitarie di Lettere Economia Diritto, Milano, 2004, p.19

digitali, nuovi sistemi per acquisire informazioni, è naturale che lì si annidino anche nuove opportunità criminali. [58]

La criminalità legata alle nuove tecnologie è stata inizialmente un ambito di studio privilegiato dell'informatica, dell'ingegneria elettronica e dei *computer security studies*, generalmente focalizzati sullo sviluppo di soluzioni tecniche finalizzate all'individuazione delle minacce all'integrità dei sistemi e alla loro protezione. Un approccio questo, si capisce, limitato agli aspetti puramente tecnici dei problemi di sicurezza, trattati separatamente dagli effetti sociali e indipendentemente dalle interazioni costanti fra tali due dimensioni.

Ed è invece lungo quest'ultima prospettiva che si iscrivono gli orientamenti elaborati dalle scienze sociali che se, da un lato, intendono approfondire la natura e le caratteristiche delle realtà criminali e delle forme di vittimizzazione associate alla Rete, consentono altresì di soffermarsi su concetti quali la devianza, il controllo sociale, il processo di valutazione delle opportunità operato da parte dei criminali informatici, capaci di soppesare il proprio agire in base ai rischi associati all'utilizzo delle tecnologie digitali. Si noti peraltro come siano non pochi gli aspetti problematici associati alle ricerche in questo ambito.

In *primis* la difficoltà di misurare prevalenza ed incidenza di suddetti fenomeni, dovuta innanzitutto alle statistiche ufficiali sulla criminalità, le quali non permettono di avere una fotografia accurata del fenomeno oggetto di studio, andando a rimarcare il cosiddetto "numero oscuro", ossia il concetto utilizzato per designare la differenza fra la criminalità "registrata" dalle agenzie del controllo sociale (a partire dai dati generati dall'attività delle forze di polizia a quelli propri della macchina processuale di giustizia penale) e quella reale, corrispondente all'insieme dei reati effettivamente perpetrati. [59]

E allo stesso modo anche le inchieste di vittimizzazione non sono immuni da criticità, si ricordi infatti come le risposte a tali indagini si basino sulla percezione degli intervistati e, in particolare, sulla loro capacità di identificare come criminale

---

58 A. Di Nicola, *Criminalità e criminologia nella società digitale,* FrancoAngeli, Milano, 2021, p. 19

59 Per una sintesi si veda Gallino L., *Dizionario di sociologia,* Utet, Torino, 2006, p. 182.

un dato evento rispetto al quale stimarsi vittima. Ora, nell'ambito della cybercriminalità, tale processo di identificazione è reso maggiormente complesso dal fatto che l'individuo può non esser conscio di essere vittima di un crimine digitale (si pensi *all'hacking*). Ancora, tale tipo di inchieste tende spesso ad attribuire agli intervistati un savoir-faire tecnologico in merito alla esperienza di vittimizzazione (ad esempio questioni sui virus informatici), competenza non necessariamente posseduta da tutti i soggetti studiati. [60]

In *secundis* si noti come la cybercriminalità, realizzandosi in parte nel cyberspazio, un ambiente per così dire "dematerializzato", lasci spesso delle tracce che necessitano, per essere interpretate, di specifiche ed altamente sofisticate competenze, che contribuiscono a lanciare una sfida sul piano della effettiva gestione del know-how tecnologico. [61]

Si può sostenere come i reati informatici, per definizione, non conoscano confini, lo spazio virtuale è invero uno spazio unitario evanescente, che sfugge cioè dal dominio di un singolo Stato: trattare di *cybercrimes* significa infatti interrogarsi su crimini dal respiro internazionale e dalla natura transnazionale, diventando così determinante, ai fini dell'applicazione delle leggi specifiche in materia, accertare da dove partano cyber attacchi ed intrusioni, come anche individuare dove si vadano ad esplicare gli effetti malevoli. La possibilità di agire da remoto permette di fatto agli autori delle condotte illecite di aggirare le sempre più fragili difese su cui possano contare gli Stati nazionali, consentendo loro di agire potenzialmente su di una dimensione planetaria. [62]

Ancora una volta si rifletta sulla portata globale del fenomeno, [63] come anche sulla sua preoccupante diffusione trasversale, per cui si palesano come necessarie tan-

---

60 G. Macilotti, op. cit. supra a nota 54, pp. 58-60

61 L. D'Alessandro, "Prefazione", in A. Pitasi (a cura di), *Webcrimes. Normalità, devianze e reati nel cyberspace,* Guerini e Associati, Milano, 2007, p. 13.

62 S. Aterno, F. Cajani, G. Costabile, D. Curtotti, *Cyber forensics e indagini digitali: manuale tecnico giuridico e casi pratici,* Giappichelli Editore, Torino, Aprile 2021.

63 Sull'estensione geografica in materia di criminalità informatica, in base ai dati offerti *dall'Internet Crime Complaint Center* nel Report 2007 inerente ai primi dieci Paesi al mondo per tali illeciti penali, al primo posto si vedono gli Stati Uniti d'America, quindi a seguire il Regno Unito, la Nigeria, il Canada, la Romania ed al sesto posto l'Italia.

to l'adozione di accordi internazionali per la prevenzione e la lotta alla criminalità informatica, quanto altresì l'idea di una cooperazione allargata fra Stati, nonché di uno sforzo globale, in un'ottica di implementazione e di armonizzazione dei vari ordinamenti interni, prevenendone eventuali situazioni di *impasse*.

Ciò che si voleva fin qui evidenziare è come lo studio delle realtà devianti associate alla Rete inviti a confrontarsi sì con fenomeni di indubbia attualità, ma altresì di difficile analisi.

In tal senso, alcuni degli strumenti e delle fonti "tradizionali" della ricerca socio-criminologica mostrano indubbiamente i loro limiti al cospetto di una criminalità caratterizzata da natura immateriale e dimensione transnazionale.

Di conseguenza nessun approccio può pretendere l'esaustività, anzi le strategie di ricerca permettono di ottenere un'immagine maggiormente accurata della cybercriminalità soprattutto qualora integrino differenti fonti e metodi di indagine, così da riuscire a far fronte a fenomeni che, per la natura stessa di Internet, presentano un carattere globale, distribuito e reticolare. [64]

3.2 Alcune precisazioni terminologiche

Si ripeta come l'evoluzione tecnologica, nonché informatica e telematica, quale fenomeno diffuso a livello globale, sia generatrice non soltanto di risultati benevoli quali di crescita sociale, di modernizzazione, di superamento di barriere ed abbattimento di distanze, di semplificazione e velocizzazione delle attività, ma altresì di sviluppo della criminalità informatica, intesa come attività illecita penalmente rilevante, commessa per mezzo ovvero contro sistemi informatici. [65]

---

64 G. Macilotti, op. cit. *supra* a nota 54, pp. 75-76

65 E. Colombo, "La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali", in *Ciberspazio e diritto: Internet e le professioni giuridiche,* Vol. 10, n. 3/4, 2009, pp. 285-304.

Se è vero infatti che il crimine accompagna l'umanità dagli albori della sua storia evolutiva, adattandosi di pari passo col variare della realtà sociale, allora in tal senso la "rivoluzione digitale" non ha fatto altro che innescare anche una sorta di "rivoluzione criminale": l'utilizzo illecito della tecnologia ha cioè generato la cosiddetta criminalità cibernetica, fenomeno in continua espansione, che ad oggi registra livelli di diffusione e pervasività tali da rendere cittadini, imprese, nonché Stati particolarmente vulnerabili. [66]

Una delle prime locuzioni utilizzate per descrivere il fenomeno in esame è quella di criminalità informatica (computer crime), che citando Ponti *"designa tutte le attività illecite in cui il computer è coinvolto come strumento, simbolo o oggetto del fatto delittuoso"*. [67] Verso la metà degli anni novanta poi, al termine evocato va affiancandosi quello di cybercriminalità (*cybercrime*), con cui si vogliono indicare tutti quei comportamenti illeciti la cui commissione implica l'uso delle reti telematiche o in cui l'autore utilizza delle conoscenze particolari del cyberspazio. [68]

In tale prospettiva, se la prima nozione si riferisce principalmente alle realtà criminali in cui è presente l'utilizzo del computer, la cybercriminalità, per come poc'anzi descritta, abbraccia un più eterogeneo insieme di condotte illecite, accomunate dall'utilizzo di Internet e realizzate attraverso un qualsiasi dispositivo che consenta la connessione in Rete. [69]

Ed è proprio quest'ultimo termine ad essersi progressivamente imposto nel dibattito pubblico e scientifico, fino ad una sua ufficiale consacrazione nell'ambito dei trattati internazionali per merito della *Convention on Cybercrime* del Consiglio d'Europa, quale primo strumento multilaterale in materia, firmato a Budapest nel 2001. [70]

---

66 P. Lorusso, *L'insicurezza dell'era digitale: tra cybercrimes e nuove frontiere dell'investigazione,* Franco-Angeli, Milano, 2011, p. 15.

67 G. Ponti, *Compendio di criminologia,* Cortina, Torino, 1994, pp. 161-163

68 Wall, S. David, *Crime and the internet,* Routledge, New York, 2001, pp.1-7

69 G. Macilotti, op. cit. *supra* a nota 54, p. 53

70 Consiglio d'Europa, *Convenzione sulla criminalità informatica,* firmata a Budapest il 23 Novembre 2001, entrata in vigore il 1 Luglio 2004.

Ciononostante l'anzidetta espressione ha patito nel tempo diverse critiche, provenienti in primo luogo dalle Nazioni Unite che non hanno mancato di sottolineare come le difficoltà di cooperazione internazionale nell'ambito del contrasto al fenomeno siano in parte legate alla natura vaga e imprecisa di tale nozione.[71] D'altronde la stessa Convenzione sulla cybercriminalità non precisa il significato di tale termine, limitandosi ad enumerarne le forme di criminalità comprese al suo interno.

Si giudica allora opportuno utilizzare tale terminologia non tanto per descrivere un fenomeno criminale a sé stante, quanto per indicare un insieme di pratiche e condotte criminali accomunate, nella loro commissione, da un ruolo centrale svolto dalle tecnologie dell'informazione e della comunicazione: differenti realtà caratterizzate da simili tratti distintivi quali: l'anonimato dei comportamenti, il carattere immateriale delle informazioni e la dimensione transnazionale delle condotte.[72]

Allo stesso modo si sono susseguite, da parte degli esperti del settore, molteplici definizioni di crimine informatico, a causa proprio della eterogeneità dei modi con cui esso può essere compiuto.

Da qui Ceccacci, in una propria definizione che richiama fortemente alla mente la proposta di Ponti: *"Il crimine informatico rappresenta qualsiasi atto o fatto contrario alle norme penali, nel quale il computer è stato coinvolto come strumento, simbolo od oggetto del fatto"*.[73]

Sul versante del diritto poi, la dottrina offre numerosi spunti classificatori.

Si può qui ricordare Sarzana e la sua suddivisione basata sullo scopo dell'azione criminosa, in:[74]

a. Crimini correlati all'utilizzo del computer ed aventi per scopo

---

71 F. Fortin, *Cybercriminalité Entre inconduite et crime organisé,* Presses internationales Polytechnique et Sûreté du Québec, Canada, 2013, p.10

72 G. Macilotti, op. cit. *supra* a nota 54, p. 54

73 G. Ceccacci, *Computer crimes,* Fag, Milano, 1994.

74 C. Sarzana, *Informatica e diritto penale*, Giuffrè Editore, Milano, 1994.

la realizzazione di un profitto per l'autore e la produzione di un danno per la vittima (si pensi tanto alla appropriazione di dati o informazioni, quanto ai crimini finanziari).

b. Crimini diretti contro il computer come entità fisica, aventi per scopo il danneggiamento parziale o totale del sistema stesso (ad esempio una immissione di programmi virus).

c. Crimini correlati con l'uso del computer diretti a provocare danni fisici ad interi gruppi o persone.

Tali premesse terminologiche si sono ritenute doverose al fine di poter successivamente trattare di attacchi informatici indirizzati a colpire le aziende sanitarie ed ospedaliere, indubbiamente atti qualificabili come minacce legate ad una criminalità del tutto "nuova", definibile cyber-dipendente.

3.3 Criminalità dipendente dalle nuove tecnologie

Le tecnologie informatiche e telematiche hanno indubbiamente fornito nuovi spazi, opportunità e strumenti di espressione alle forme di criminalità più "tradizionali", a tal proposito McGuire e Dowling parlano invero di criminalità cyber-abilitata. [75]

Si considerino, a fini esemplificativi, il furto e le frodi di identità: certo è sempre stato possibile appropriarsi di informazioni relative all'identità altrui, fingersi un'altra persona ed ingannare terzi per trarne illeciti vantaggi. Ma tale reato, che nel mondo fisico era dote di pochi poiché richiedeva un agire scaltro, qualificato, nonché sofisticato, ad oggi risulta maggiormente realizzabile nonché pericoloso. Ciò è dovuto al fatto che si possono agevolmente sottrarre informazioni personali

75 M. McGuire, S. Dowling, *Cybercrime a review of the evidence. Research report 75, Home Office,* Londra, 2013.

altrui online, magari tramite social media, e servirsene materialmente per produrre documenti fisici da presentare nei contesti più disparati al fine di ottenere benefici ed illeciti vantaggi. [76]

Eppure l'avvento della società digitale ha anche contribuito all'emergere di condotte illecite del tutto nuove, ad alto contenuto tecnologico ed interamente associate alla Rete: sono i veri crimini informatici, quelli puri, che compaiono con Internet e possono essere perpetrati solo all'interno del cyber-spazio, come afferma Wall nella sua elaborazione. [77]

A tal proposito ci si rifà alla definizione di criminalità cyber-dipendente, in merito alla quale McGuire e Dowling hanno avanzato due sotto-classificazioni basate sul modo in cui tali crimini sono realizzati.

Per i due autori infatti i crimini dipendenti dalle nuove tecnologie rientrerebbero in due famiglie principali: quella delle intrusioni illecite nelle reti informatiche e quella dell'interruzione o del danneggiamento della funzionalità dei computer e delle reti. [78]

Così un chiaro esempio annoverabile nella prima famiglia risulta essere l'hacking, quale accesso non autorizzato a reti informatiche, computer, telefoni cellulari e dispositivi che, sfruttando lacune di sicurezza, mira a raccogliere principalmente dati personali od informazioni utili.

Si pensi al valore di un dato sanitario, fornito dall'insieme di dati anagrafici (nome, cognome, codice fiscale etc.) utilizzabili per furti di identità, uniti ai dati sulle patologie, impiegabili per attività di marketing farmaceutico o altre attività commerciali collegate.

Della seconda famiglia invece fanno parte i *malware* (software maligni finalizzati a diffondersi nei computer ostacolandone il funzionamento, passibili di assume-

---

76 A. Di Nicola, op. cit. *supra* a nota 58, p. 41

77 D. S. Wall, "Digital realism and the governance of spam as cybercrime", in *European journal on criminal policy and research*, 10(4), 2005.

78 A. Di Nicola, op. cit. *supra* a nota 58, p. 37

re diverse forme quali *virus,* [79] *worm,* [80] *spyware,* [81] *ransomware* [82]); lo spam (quali messaggi di posta elettronica non richiesti, inviati tipicamente a innumerevoli destinatari, al fine di raccogliere dati personali delle vittime); il *Denial-of-Service* (DoS), quale attacco consistente nell'inviare intenzionalmente grandi quantità di dati ad un obiettivo mirato, innescandone così un crash, al fine di impedire agli utenti legittimi di accedere ed utilizzare la risorsa di rete; il *Distributed Denial-of-Service* (DDos), cioè uno speciale DoS che si muove non da un indirizzo IP unico ma da più di uno, anzi spesso migliaia.

Nel suddetto complesso di cyber-condotte riveste, come si vedrà, ruolo di considerevole importanza l'attacco ransomware: per ovvi motivi, strutture come ospedali e cliniche di rado possono permettersi periodi di disservizio causati da cyber-attacchi. Pertanto i criminali informatici, profittando di tale vulnerabilità, sfruttano l'importanza vitale di tali strutture come leva per forzare il pagamento di ingenti somme di denaro, quale riscatto, per fornire alle vittime la chiave atta a decrittografare tutti i dati sensibili precedentemente presi in ostaggio e per riottenere il regolare ripristino del sistema. Ancora si consideri come, in un loro saggio, Brar e Kumar [83] propongano una minuziosa classificazione circa gli attacchi informatici, basata sull'impatto che essi possono registrare sui tre principi fondamentali della cyber-sicurezza: la confidenzialità, l'integrità e la disponibilità, su tali nozioni risulta necessario soffermarsi per brevi cenni.

---

79 I virus sono software che possono causare da lievi disfunzioni al computer sino ad effetti notevolmente gravi in termini di danneggiamento o cancellazione di file, software, o hardware. Si auto-replicano all'interno dei computer e fra i computer, e hanno sempre bisogno di un ospite (quale un file) che agisca come portatore. Per infettare un computer necessitano comunque di una azione umana, consistente nell'eseguire o aprire il file infetto.

80 I worm sono programmi auto-replicanti che possono diffondersi autonomamente all'interno e tra i computer, senza un ospite o alcune azione umana

81 Lo spyware è un software che invade la privacy degli utenti raccogliendo informazioni sensibili o personali dai sistemi infetti e monitorando i siti web visitati. Tali informazioni possono poi essere trasmesse a terze parti.

82 Il ransomware è un tipo di virus che prende il controllo del computer di un utente ed esegue la crittografia dei dati, impedendo, una volta installato, agli utenti di accedere ai propri dati che risiedono nel computer o di usare la macchina stessa. Di regola viene chiesto un riscatto per ripristinarne il normale funzionamento.

83 H. Brar, G. Kumar, "Cybercrimes: a proposed taxonomy and challenges", in *Journal of computer networks and communication,* 2018.

3.3.1 La triade CIA della sicurezza informatica

Innanzitutto tramite la nozione di "sistema informatico" si suole intendere l'insieme delle risorse computazionali, di comunicazione (quali le reti locali), nonché di tutte le informazioni trattate dalle anzidette risorse.

Parlando di sicurezza informatica invece si intende, secondo la definizione fornita dall'ISO *(International Standard Organization),* l'insieme delle misure atte a garantire, ad un sistema informatico, le seguenti proprietà: confidenzialità, l'integrità e disponibilità.

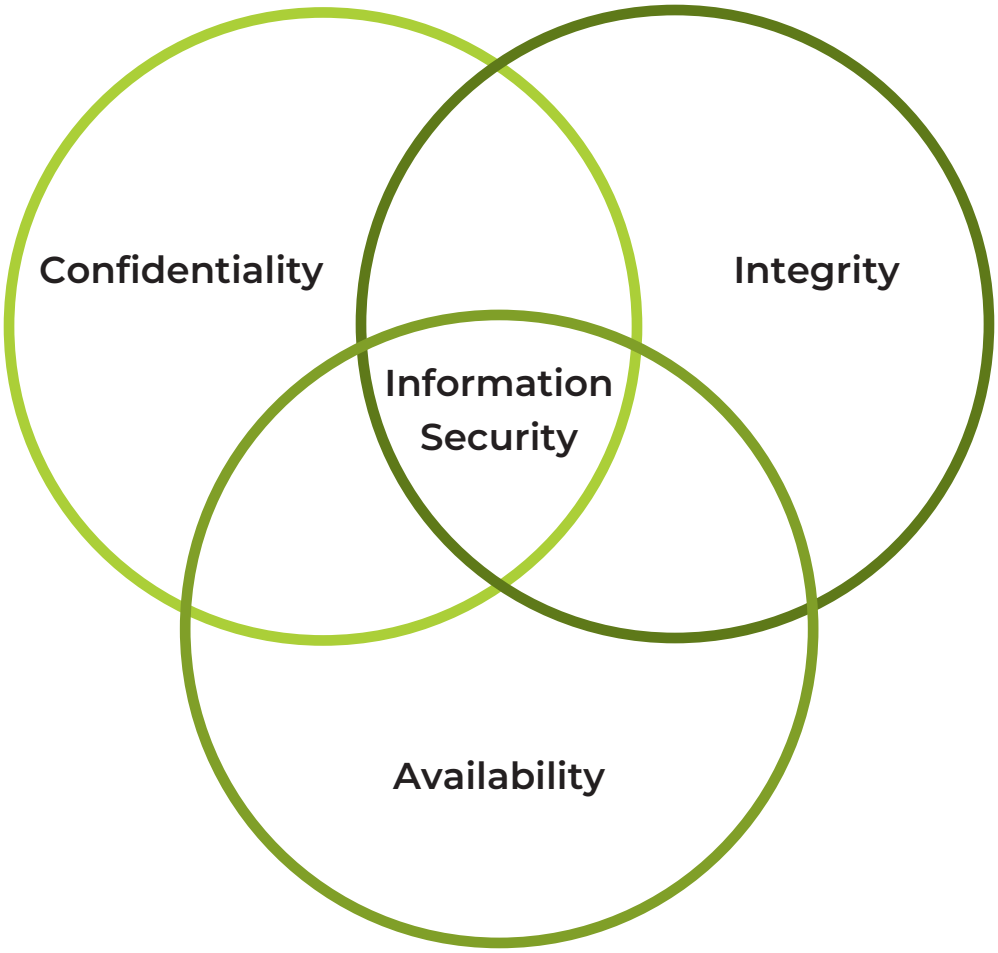

Figura 3.1: La sicurezza informatica secondo la definizione ISO

Tali principi guida si figurano come le tre componenti principali della cosiddetta triade CIA *(Confidentiality, Integrity e Availability)* per *l'Information Security,* un modello di sicurezza delle informazioni ampiamente accettato, condiviso ed altresì destinato a guidare le procedure e politiche di sicurezza di qualsivoglia organizzazione.

Si capirà, un'eventuale compromissione di qualsiasi elemento della triade comporterebbe inevitabilmente la diretta compromissione della stessa sicurezza dei dati.

Nel prosieguo della trattazione si vogliano schematicamente riassumere i tre principi guida e le macro-raccomandazioni che ognuno di essi comporta:[84]

La confidenzialità innanzitutto ha a che fare con il mantenere privati i dati di una organizzazione: pare ovvio, meno persone possono accedere ad essi, minore sarà il rischio che possano essere effettuate violazioni della sicurezza. Ciò implica che il patrimonio informativo (detto asset) sia passibile di accesso solo da parte dei soggetti in possesso di una adeguata autorizzazione, tramite cui questi stessi potranno leggere, stampare, copiare o esser semplicemente a conoscenza dell'esistenza di una determinata risorsa.

Al fine di mantenere i dati riservati si dovranno allora mettere in atto protezioni che siano appropriate, alcune delle quali dovrebbero essere presenti nativamente all'interno dei sistemi di gestione dati, si pensi ad esempio a tutto ciò che riguarda le regole di autenticazione e autorizzazione nell'accesso ai dati. Ancora, si può parimenti garantire una maggiore confidenzialità adottando meccanismi di crittografia: metodo efficace per proteggere e rendere sicure le informazioni, tramite loro conversione in testi cifrati di modo che solo i soggetti autorizzati possano decrittografarli, impendendone al contempo accessi esterni non autorizzati.

Per esemplificare, un attacco informatico diretto a minare la confidenzialità risulta essere il *keylogger*, un tipo di malware che opera sullo sfondo di un sistema informatico, in modalità nascosta, di modo che tutte le informazioni inserite

---

84 G. Me, "La sicurezza dei sistemi informatici aziendali", in *Tecnologie dell'informazione e comportamento devianti,* Milano, 2004, pp. 101-135.

dall'utente vengano catturate e trasmesse all'aggressore, senza che l'utente stesso autorizzato ne abbia consapevolezza.

L'integrità mira a garantire invece che i dati siano mantenuti in uno stato corretto, che non vengano manomessi e che dunque risultino affidabili. Oltre a controllare l'accesso ai dati invero le misure di sicurezza dovrebbero anche limitare ciò che le persone possono fare coi dati stessi: l'asset informatico potrà essere modificato cioè solo tramite autorizzazione (la possibilità ad esempio di spostare, copiare, alterare i dati verrà limitata). Ed è proprio tale autorizzazione ad individuare un livello di accesso alle risorse a cui sono associate un insieme definito di operazioni permesse: ad esempio, un utente potrebbe accedere in lettura ad un file, ma non in scrittura.

Esemplificando, un attacco diretto all'integrità può essere il *data diddling,* ovvero una alterazione, una manipolazione illegale o non autorizzata dei dati, e nel caso in cui i nuovi dati sovrascrivano i precedenti senza lasciare traccia, il danno risulterebbe irreversibile, a meno che non vi siano copie di sicurezza adeguate.

La disponibilità infine implica che i dati siano costantemente disponibili per gli utenti autorizzati, ogni qualvolta essi lo richiedano, ciò racchiude il dover mantenere sistemi, reti e dispositivi sempre attivi e funzionanti, di modo che la data organizzazione possa continuare ad operare anche di fronte ad un attacco informatico, o che non si renda ad ogni modo indisponibile a causa di guasti, malfunzionamenti, errori umani, calamità naturali etc.

Per garantire la disponibilità le organizzazioni dovranno utilizzare reti, server, storage, meccanismi di replica e protezione dati, nonché dotarsi di opportuni piani di *backup/recovery* per rispristinare l'operatività e la disponibilità di un sistema.

Tipici attacchi alla disponibilità risultano essere il DoS ed il DDoS, per mezzo dei quali i criminali si introducono illecitamente nelle reti informatiche e/o interrompono o danneggiano la funzionalità di computer e reti.

Chiare appaiono le conseguenze laddove il target dell'attacco sia una struttura ospedaliera ed oggetto della compromissione siano proprio i server dell'infrastruttura informatica: gravi problemi tecnici, disservizi nell'accesso dei pazienti

alla stessa struttura, possibilità di eseguire prestazioni ospedaliere solo attraverso modulistica cartacea, con tutto ciò che ne consegue in tema di qualità dell'assistenza, nonché tempestività delle cure e/o di soccorso.

Date tali conseguenze devastanti ed impattanti non solo sui sistemi sanitari, ma anche su ciò che più propriamente attiene alla salute dei pazienti, le strutture ospedaliere dovrebbero iniziare a considerare in via proattiva e preventiva la sicurezza dei propri sistemi informatici, al fine di proteggere adeguatamente, e fin dalla progettazione del sistema, non solo i dati sanitari in essi conservati, ma anche l'operatività dei servizi.

Si tornerà comunque sull'argomento nell'avanzare della trattazione, ma già in questa sede si può anticipare come consapevolezza, formazione ed investimenti in termini di sistemi e di personale specializzato possano costituire elementi portanti di un piano strategico adottabile da parte delle strutture ospedaliere al fine di tutelarsi al meglio nei confronti dei rischi derivanti dalle cyber-compromissioni.

3.3.2 Sette principi di sicurezza

Si vogliano ora passare celermente in rassegna sette principi generali sulla sicurezza, di natura non tecnica, ma anzi di carattere generale, evolutisi nel tempo sino a diventare largamente accettati nonché fondamenta per la costruzione di sistemi sicuri e codificati, quali i sistemi operativi. [85]

Essi sono:

a. Minimo privilegio: è probabilmente uno dei principi fondamentali della sicurezza delle informazioni, indica come ogni risorsa (informatica, umana etc.) debba avere soltanto le autorizzazioni di cui ha bisogno per compiere il proprio lavoro,

---

85 J. Saltzer, "The protection of Information in Computing System", in *Proceedings of the IEEE,* v. 63 n.9, 1975, pp. 1278-1308.

nulla di più. Così ad esempio ad un utente verranno concessi livelli, o permessi, minimi di accesso, nei limiti in cui siano necessari per svolgere le proprie mansioni;

b. Difesa in profondità: suggerisce come non si debba far affidamento soltanto su di un unico meccanismo di sicurezza, per quanto questo sia ritenuto estremamente valido ed affidabile. L'adozione infatti di molteplici sistemi di sicurezza che siano in grado di coprire eventuali malfunzionamenti di altre contromisure consente proprio di evitare la compromissione dell'intero sistema;

c. Anello debole: la sicurezza, proprio in forza del principio previamente enunciato, è rappresentabile come una catena di contromisure tanto forte quanto l'anello più debole: chiunque intenda attaccare il sistema lo farà infatti nella parte maggiormente vulnerabile, ovvero quella con la contromisura più fragile;

d. Fallimento in regime di sicurezza: quando una contromisura fallisce, lo deve fare comunque in maniera "sicura". Ciò significa che se un sistema di sicurezza ha un malfunzionamento, non dovrà ad ogni modo consentire l'accesso ad eventuali intrusi, anche a costo di negare l'accesso stesso ai legittimi utenti;

e. *Security through obscurity:* è un principio largamente seguito nella vita di tutti i giorni e allude al voler proteggere gli oggetti, nascondendoli. In campo informatico si riferisce al mantenere segrete le informazioni relative ad un sistema di sicurezza, si tenga comunque bene a mente che è una tattica da accompagnarsi necessariamente ad una reale protezione adottata, altrimenti da sola risulterebbe inefficace;

f. Semplicità: principio che richiede di dotarsi di strumenti di semplice utilizzo e, per quanto possibile, anche di semplice

progettazione, ciò invero consente una larga e veloce comprensione di ciò che accade, rendendo molto più facile capire se si è concretamente sicuri;

g. Partecipazione universale: la maggior parte dei sistemi di sicurezza richiede infatti la partecipazione universale (o, almeno l'assenza di opposizione attiva) delle risorse umane coinvolte. Di qui l'importanza di un corretto training in ambito di politiche di sicurezza: i dipendenti sono infatti la prima e la più forte linea di difesa contro la stessa criminalità informatica. Questo perché ancora numerosi attacchi informatici si basano sul trarre in inganno o sul convincere vittime mirate a compiere qualcosa che non dovrebbero (fare click su di un collegamento infetto od aprire un allegato di posta elettronica sospetto), invece con una corretta formazione del personale suddetti tentativi di manipolazione potrebbero essere agilmente individuati e segnalati ai corrispondenti team di sicurezza.
A tal proposito si richiamano a seguire le parole di Pierguido Iezzi, CEO e fondatore della cybersecurity company Swascan: "Imparare a riconoscere e-mail e messaggi sospetti è assolutamente vitale per la tenuta di qualsiasi organizzazione.[...] Per farlo è consigliabile implementare regolari e periodiche sessioni di formazione nei confronti di queste minacce. La migliore tecnologia, infatti, è inutile se non è affiancata ad un lavoro di riduzione del rischio umano." [86]
Il tema *dell'awareness* dunque, ovvero il grado di conoscenza e formazione dei dipendenti rimane ad oggi un punto fermo, sicuramente al pari di quello della resilienza e della resistenza tecnologica.

---

86 Intervista a Pierguido Iezzi, pubblicata il 14.05.2022, ad opera di Massimo Canorro, sul quotidiano sanitario nazionale Nurse24.

3.4 Nuovi autori: i cyber-criminali

Le dimensioni del fenomeno dei *computer crimes* destano ormai notevole allarme sociale, le manifestazioni patologiche legate all'uso dell'informatica si vanno moltiplicando, studi, ricerche, dibattiti e statistiche evidenziano sempre più che il problema esiste e che sta assumendo dimensioni sempre più vaste. Sembra esser necessario applicare nell'analisi del fenomeno un approccio multidisciplinare: ossia uno sforzo congiunto di ricerca da parte di criminologi, scienziati dell'informazione ed esperti di cyber-sicurezza. Oltre all'analisi su natura e caratteristiche delle nuove condotte criminose legate al mondo digitale, la letteratura criminologica si è a lungo soffermata anche sullo studio in merito al profilo dei criminali informatici.

Risulta in questa sede interessante ricordare la comparazione operata da Weulen Kranenbarg fra l'autore di criminalità cyber-dipendente ed il criminale tradizionale. [87] Da tale analisi si ricavano le seguenti considerazioni: [88]

a. I reati cyber-dipendenti garantiscono l'anonimato, mentre ciò non viene altrettanto assicurato nei reati tradizionali;

b. I cybercriminali hanno una minore probabilità di essere scoperti e perseguiti rispetto ai criminali tradizionali, con conseguenti tassi di arresto notevolmente più bassi;

c. Le conseguenze sociali negative derivanti dalla commissione di un crimine cyber-dipendente sono molto meno pesanti. Ciò è dovuto al fatto che l'ambiente sociale può non essere consapevole del comportamento tenuto online da parte del criminale informatico che perciò non si attende di per sé alcuna conseguenza sociale negativa per le proprie condotte illecite;

---

87 M. Weulen Kranenbarg, "Contrasting cyber-dependent and traditional offenders. A comparison on criminological explanations and potential prevention methods", in E.R. Leukfeldt, T. Holt (a cura di), *The Human factor of cybercrime,* Routledge, Londra, 2020, pp.194-215.

88 A. Di Nicola, op. cit. *supra* a nota 58, p. 62

d. Chi agisce nel mondo digitale si sente in qualche modo disconnesso dal mondo fisico, il contesto digitale infatti può portare ad un fenomeno definito da Suler "disinibizione online". [89] Il cybercriminale potrebbe dunque non sentire alcuna responsabilità per aver commesso azioni illecite online, specialmente se si tratta di crimine cyber-dipendente, dove l'obiettivo principale è un computer e la vittima umana dietro a quel computer può essere totalmente sconosciuta;

e. Le opportunità, come già si è intuito, per i criminali cyber-dipendenti si manifestano in situazioni completamente diverse rispetto a quanto avviene per i criminali tradizionali;

f. Sono necessarie svariate competenze di diversa natura, alcune essenziali al fine di commettere crimini cyber-dipendenti. Va tuttavia ricordato che anche individui che siano provvisti di minori competenze informatiche possono sempre di più perpetrare reati altamente tecnici, in conseguenza del diffondersi del *"cybercrime-as-a-service"* (servizi e kit "pronti all'uso" acquistabili per portare avanti attacchi complessi anche senza il *know-how* tecnico necessario);

g. È indubbio che servano pazienza e scrupolosità per ottenere tali abilità tecniche specifiche. Mentre è stato dimostrato come la maggior parte dei criminali tradizionali non abbia un alto livello di autocontrollo e disciplina, ciò non è altrettanto vero per i criminali cyber-dipendenti, i quali devono spesso investire lunghi periodi di tempo nell'acquisizione di competenze altamente specialistiche.

Una lacuna presente nella letteratura criminologica attuale risulta essere la mancanza di indagini approfondite su come gli autori di criminalità fisica-tradizionale

---

89 J. Suler, "The Online Disinhibition Effect", in *Cyberpsychology & behavoir,* 7(3), pp. 321-326.

facciano uso dello spazio digitale, o semplicemente della tecnologia per la commissione dei loro reati offline. Nessun ricercatore poi si interroga sugli spostamenti, più o meno possibili, dei criminali tra lo spazio fisico e quello propriamente digitale: non ci sono cioè tracce di lavori scientifici incentratisi su come un attore tradizionale, ad un certo punto possa intraprendere una carriera criminale online e sul ruolo delle competenze digitali, tecnologiche, nonché informatiche in questo tipo di spostamenti.

Ed è proprio rispetto a tale tema che si può prendere in considerazione il periodo pandemico da Covid-19, quale fenomeno sociale totalizzante, che è stato in grado di toccare e plasmare ogni aspetto della vita umana organizzata.

A fronte infatti di una generale e decisa contrazione della criminalità tradizionale, specialmente appropriativa, gli anni pandemici (il 2020 e il 2021) sono stati spettatori di un forte ed incontrollato aumento della criminalità legato al mondo online, in tutti i Paesi industrializzati: la crisi sanitaria mondiale ha, in altri termini, innescato una sorta di "criminalità digitale pandemica", aggressiva, predatoria, ed anche organizzata. [90] Ovvio è che fra i suoi effetti la pandemia abbia messo in luce come la sanità di per sé sia estremamente frammentata e vulnerabile: il forte stress che ha colpito il personale medico, l'esigenza di velocizzare ed intensificare il processo di trasformazione digitale, ritenuto ormai indispensabile, e la necessità di rispondere prontamente all'emergenza, hanno senza dubbio messo a dura prova tutti i sistemi sanitari.

Si tornerà approfonditamente sul tema nel discorrere dei prossimi capitoli ma già qui si noti come si sia assistito in tale periodo ad una escalation di attacchi informatici contro ospedali, strutture sanitarie e società biotecnologiche: i cyber-criminali hanno opportunisticamente fatto leva sul senso di instabilità e di incertezza generato dalla pandemia, lanciando ripetute aggressioni proprio nel momento in cui tutte le risorse erano concentrate sul salvataggio di vite umane e sulla gestione di un flusso di pazienti di gran lunga superiore rispetto alle capacità ricettive ordinarie.

---

90 A. Di Nicola, op. cit. *supra* a nota 58, pp. 65-66

Nel concludere tali generali, quanto necessarie, considerazioni, si voglia sottolineare come la pandemia, quale esperimento naturale criminologico, abbia chiarito che è il livello di digitalizzazione diffuso a determinare il posizionamento della criminalità e dei suoi autori lungo lo spettro della criminalità digitale, e che questi riposizionamenti lungo tale spettro da parte degli stessi autori criminali possono avvenire molto rapidamente.

Sempre più allora, la ricerca criminologica si dovrà occupare di criminali posizionati lungo lo spettro della criminalità digitale ed in particolare di tutte quelle variabili soggettive ad essi riferite che possono in qualche modo andare ad influenzare il loro collocarsi in una posizione piuttosto che in un'altra lungo lo spettro stesso.

Di certo si può annoverare come ulteriore fattore caratterizzante i crimini informatici tutti una analisi circa le tipologie, le caratteristiche, l'evoluzione dei cyber-autori coinvolti, e di conseguenza in materia di innovative forme di schemi criminali associativi che si stanno nel tempo via via evidenziando. Si vogliano approfondire tali tematiche proprio nell'immediato prosieguo della trattazione.

3.5 Dagli hacker alle cyber-gang

"Il termine hacker indica l'esplorazione intellettuale a ruota libera delle più alte e profonde potenzialità dei sistemi di computer, o la decisione di rendere l'accesso ai computer stessi ed alle informazioni quanto più libera ed aperta possibile", così Bruce Sterling, uno dei padri della letteratura *cyberpunk*,[91] nella sua opera, a metà fra narrativa e saggistica, *"The hacker Crackdown",* con cui ritraeva il mondo della Rete degli anni Novanta. [92]

---

91 Il Cyberpunk è un genere narrativo, affermatosi negli Stati Uniti nel corso degli anni Ottanta, in cui i temi legati alla realtà delle società post-industriali (robotica, realtà virtuale, cibernetica, telematica etc.) vengono elaborati in chiave fantastica nel segno di una ideologia contestataria, di ribellione e di critica sociale.

92 B. Sterling, *Giro di vite contro gli hacker* (The hacker crackdown), Shake Edizioni Underground, Milano, 1996.

La storia *dell'hacking* ha inizio nell'inverno tra il 1958 e il 1959, grazie alle prime "esplorazioni" tecnologiche degli studenti del *Massachussetts Institute of Technology* (MIT) di Cambridge, più precisamente in un club studentesco di modellismo ferroviario *(Tech Model Railroad Club)*, al cui interno per la prima volta cominciò a circolare il termine di *"hacker"*.[93] Quest'ultimo aveva in origine una connotazione del tutto positiva: nel gergo usato dai membri del club soleva indicare tutti coloro che erano dotati di eccezionali abilità informatiche, capaci di "spingere" i programmi al di là delle funzioni per le quali erano stati progettati (come peraltro, il significato del verbo *to hack*).[94]

Ed è proprio al MIT che nel 1959 furono istituiti i primi corsi di informatica, dedicati allo studio del linguaggio di programmazione, e dove giunsero i primi *mainframe* (ossia elaboratori in grado di archiviare una grande mole di dati ed eseguire prestazioni molto complesse), grazie ai quali gli hacker poterono per la prima volta operare direttamente sulle macchine. Si trattava dunque di questo: un gruppo di studenti brillanti, intelligenti e versatili, che dedicarono anima e corpo all'informatica, con l'obiettivo, sentito quale sfida tecnologica, di realizzare programmi sempre migliori utilizzando il minor numero possibile di istruzioni e righe di codice. Gli eccezionali risultati ottenuti convinsero i protagonisti di quella prima rivoluzione informatica che nozioni come il libero accesso alle informazioni, la disponibilità della tecnologia e l'utilizzo dei computer, potessero consentire di apportare miglioramenti alla società tutta.[95]

Per i precursori del MIT dunque, i principi ed ideali sui quali si basava la pratica *dell'hacking* erano i seguenti:

a. l'accesso ai computer ed alle reti deve essere libero ed illimitato;

---

93 I. Corradini, C. Di Fede, "Hacker e internet crime", in G. Marotta (a cura di), *Tecnologie dell'informazione e comportamenti devianti,* Edizioni Universitarie di Lettere Economia Diritto, Milano, 2004.

94 Si riportino le parole di S. Levy, "Hacker, gli eroi della rivoluzione informatica", Shake Editore, Milano, 1996: *"La tecnologia era il loro parco giochi. I membri anziani stavano al club per ore, migliorando costantemente il sistema, discutendo sul da farsi, sviluppando un gergo esclusivo, incomprensibile per gli estranei che si fossero imbattuti in questi ragazzi fanatici con le loro camice a maniche corte a quadretti e matita nel taschino".*

95 G. Pomante, *Hacker e computer crimes,* Volume 41/15, Edizioni Simone, Napoli, 2000, pp. 22-29.

b. lo scambio delle informazioni privo di ostacoli è una essenziale libertà e nessuna considerazione di natura politica, economica e tecnica deve impedire l'esercizio di tale diritto fondamentale;

c. i sistemi informatici possono contribuire al miglioramento della società, grazie alla loro capacità di diffondere le informazioni in modo veloce e capillare.

d. le informazioni stesse sono considerate patrimonio dell'umanità, al pari delle risorse naturali, e pertanto, ove vengano imbrigliate o filtrate dai governi al fine esercitare il controllo sulla collettività, queste dovranno essere recuperate e diffuse.

È da qui che trae origine l'etica hacker, assieme ad una loro raffigurazione prettamente "romantica": mossi da quella che essi stessi definiscono *un'eroica passione antiburocratica*, gli hacker aspirano ad ergersi quali paladini di una informazione libera e priva di condizionamenti esterni. Pertanto i sistemi protetti da misure di sicurezza non vengono violati col fine di danneggiarli o provocarne un malfunzionamento, ma per recuperare e diffondere le informazioni in essi contenute. [96]

La caratteristica pertanto che più appare permeare la complessa struttura psicologica degli hacker è proprio il sentimento di onnipotenza derivante dal rapporto instaurato col computer: il controllo completo di *hardware e software,* la consapevolezza di poter dominare pienamente la tecnologia e di poterla sfruttare per portare a termine qualsiasi iniziativa, radicano negli hacker la convinzione di appartenere ad un corpo d'élite, così infatti Bruce Sterling nella sopracitata opera: *"quando si è un hacker è l'intima convinzione di appartenere ad un'élite ciò che autorizza a violare le regole, o piuttosto a trascenderle"*.

Può essere qui di interesse ricordare il breve quanto eloquente monologo pubblicato nel 1986, intitolato *"The Conscience of a hacker"* (conosciuto anche come

---

96 *Ivi*, pp. 30-37

"The hacker Manifesto") scritto da Loyd Blankenship, hacker statunitense, passato alla storia con lo pseudonimo di *The mentor,* il quale fu membro della *Legion of Doom,* uno dei gruppi più famosi dell'underground digitale degli anni Ottanta. [97]

Suddetto saggio viene considerato una pietra miliare della cultura hacker, d'altronde presenta innumerevoli spunti di riflessione relativamente agli aspetti psicologici dei primi hacker: la passione, la curiosità , la sete di conoscenza per una realtà che chiede solo di essere esplorata, la frustrazione di vivere in un mondo imperfetto che priva di informazione e risorse chi vuole elevarsi sopra la media, l'idea di appartenere ad una distinta e peculiare comunità, quella che popola il ciberspazio e che combatte una propria "battaglia" sulla "frontiera elettronica", ed ancora uno spirito fortemente antiautoritario ed antiburocratico, come anche l'avversione per tutto ciò che viene sentito come imposto, quali le facili etichette. [98]

Il passo tuttavia sarà alquanto breve nel transitare verso una connotazione di hacker del tutto negativa: passando da *"eroi della rivoluzione informatica"* secondo Steven Levy, a criminali informatici *tout court* secondo i mass media, l'opinione pubblica ed altresì l'immaginario collettivo. [99] Il timore e l'apprensione per gli hacker sembra ormai diffondersi con impeto in tutto il globo: la facilità con cui

---

97 M. Warren, S. Leitch, "Hackers Taggers: A new type of hackers", in *School of Information Systems, Deakin University press, Springer,* 7 August 2009, pp. 425-431.

98 The Mentor, The conscience of a Hacker, e-zine Phrack, Volume 1, Issue 7, Phile 3, 8 January 1986: *" […] Ma avete mai guardato dietro agli occhi di un hacker? Non vi siete mai chiesti cosa abbia fatto nascere la sua passione? Quale forza lo abbia creato, cosa può averlo forgiato? Io sono un hacker, entrate nel mio mondo. Il mio è un mondo che inizia con la scuola. Sono più sveglio di molti altri ragazzi, quello che ci insegnano mi annoia. […] Ho fatto una scoperta oggi, ho trovato un computer. Fa esattamente quello che voglio. Se commetto un errore, è perché io ho sbagliato, non perché io non gli piaccio. […] Questo è il luogo a cui appartengo, io conosco tutti qui, non ci siamo mai incontrati, non abbiamo mai parlato faccia a faccia, non ho mai ascoltato le loro voci, però conosco tutti. […] Ora è questo il nostro mondo. Noi facciamo uso di un servizio già esistente che non costerebbe nulla se non fosse controllato da approfittatori ingordi, e voi ci chiamate criminali. Noi esploriamo, e ci chiamate criminali. Noi cerchiamo conoscenza, e ci chiamate criminali. […] Voi costruite bombe atomiche, finanziate guerre, uccidete, ingannate e mentite, e cercate di farci credere che lo fate per il nostro bene, e poi siamo noi i criminali. Si, io sono un criminale. Il mio crimine è la mia curiosità. Il mio crimine è quello di scovare qualche vostro segreto, qualcosa che non vi farà mai dimenticare il mio nome. Io sono un hacker e questo è il mio manifesto. Potete anche fermare me, ma non potete fermarci tutti , dopo tutto, siamo tutti uguali."*

99 Così Steven Levy: *"Il problema cominciò con arresti molto pubblicizzati di adolescenti che si avventuravano elettronicamente in territorio digitali proibiti […] la parola hacker divenne rapidamente sinonimo di "trasgressore digitale", e con la comparsa dei virus informatici fu letteralmente trasformato in una "forza del male".*

appare possibile portare a termine una azione delittuosa per mezzo di un elaboratore è difatti la spinta che porta numerosi soggetti a delinquere.

L'indirizzare se stessi verso la carriera criminale non è dunque un *raptus* momentaneo, od un salto improvviso, ma anzi si figura quale un avvicinamento progressivo: una presa di coscienza graduale delle potenzialità dello strumento informatico, che conduce lentamente l'individuo a valutare l'opportunità di perpetrare il crimine restando impunito, fino a raggiungere la piena convinzione di riuscire a rendersi irreperibili, sfruttando l'anonimato, e di non essere in alcun modo perseguibili.

È da qui che prendono il via diverse elaborazioni teoriche circa possibili classificazioni riguardanti le tipologie di hacker esistenti, basate sulle tecniche di intrusione utilizzate e sulle motivazioni che le sottendono.

Si elenchi a seguire la tassonomia delineata dal criminologo M. Strano: [100]

a. Hacker distruttivo vandalico: il suo agire risulta caratterizzato da operazioni di danneggiamento operate mediante l'impiego di virus, che comportino una corruzione dei dati, una loro cancellazione, o ancora il blocco generale del sistema operativo. La motivazione sottostante a condotte di tal genere è paragonabile, per certi versi, a quella di certe forme di violenza contro le cose e le persone, ossia apparentemente senza un vero e proprio vantaggio pragmatico per l'autore, ma anzi per pura valenza comunicativa indirizzata sia verso l'ambiente esterno, mostrando agli altri cosa si è in grado di fare, sia verso il sé dell'autore, infondendosi così un intimo senso di autostima.

b. Hacker distruttivo professionista: le intrusioni, seppur nuovamente caratterizzate di finalità distruttive e operate tramite l'utilizzo di virus informatici, sono sorrette in tal caso da una logica di tipo pragmatico-utilitaristica, nonché lucrativa: l'ac-

---

100 M. Strano, opera citata *supra* a nota 267, pp. 56-60.

cesso illegale costituisce infatti una opportunità di effettuare un danneggiamento programmato, che sia su commissione, e che venga retribuito da una entità antagonista a quella proprietaria del sistema danneggiato (aziendale, politica, militare etc.).

c. Hacker tradizionale: per questa categoria le intrusioni rappresentano per lo più un vezzo o un gioco, oltre ad un sistema per dimostrare a sé e agli altri la perizia acquisita in campo informatico. Alla base dall'agire non risiede dunque una motivazione di lucro, quanto piuttosto il "gusto della sfida", come anche una certa ostilità verso gli "steccati normativi", sentiti come imposizioni da parte dei detentori della leadership tecno-giuridica.[101]

d. Hacker spia: per questa figura l'attività di intrusione illecita è legata alla sottrazione, sempre su commissione, di informazioni circolanti sulle reti telematiche o memorizzate all'interno di sistemi informatici. Ovvio è che le informazioni costituiscano uno dei beni di maggior valore nella società terziarizzata, in campo aziendale, militare ed istituzionale, così un hacker un grado di "bucare" e penetrare in un determinato sistema può senza dubbio imbattersi in notizie che siano di ingente valore.

e. Hacker antagonista: si tratta di una tipologia di hacker animata da forti spinte motivazionali ideologiche: i c.d. "tecnocrati capitalisti" gestiscono il potere tramite la creazione di banche dati virtuali, dove concentrano informazioni di natura politica, economica e giudiziaria, impedendone l'accesso al popolo, che rimane così in una condizione di inferiorità.
Per contrastare tale stato di cose l'hacker antagonista progetta e porta a compimento alcune tattiche di sabotaggio elet-

---

101 Ne è un esempio il caso di Tappan Morris, studente americano di ventidue anni della Cornell University che, nel 1988, mise "per gioco" su internet un virus da lui scritto che, nel giro di poche ore, bloccò più di 6000 computer, compreso quello della NASA e dell'US Air Force.

tronico, in particolare mediante l'introduzione di virus e tramite varie tecniche di *cracking* dei sistemi centralizzati, una sorta di "guerriglia virtuale" combattuta nel ciberspazio.

Tuttavia di indifferibile necessità appare ora tracciare un sommario profilo circa le nuove ed odierne forme di criminalità informatica.

Invero episodi criminali che un tempo erano esclusivo appannaggio di soggetti dotati di elevate capacità tecnico-informatiche, operanti in forma isolata ed autonoma, e spesso, come si è visto, senza alcuna diretta finalità di lucro, ad oggi vengono ricondotti sempre più a composite organizzazioni che, ricorrendo a specifiche forme di arruolamento di indispensabili esperti tecnici, gestiscono fila di "imprese" che assicurano enormi introiti finanziari, delineandosi così nuovi schemi associativi e modelli strutturali criminali, dalle sfumature marcatamente transnazionali. [102]

In sostanza il profilo del delinquente informatico sembra ormai discostarsi dalle figure "classiche" dei sopracitati hackers, o meglio *crackers*, [103] tipiche del primo evo della criminalità informatica, per indirizzarsi piuttosto verso innovative fenomenologie, da collocare in più ampi contesti di associazionismo criminale.

Ovvio è che le sempre più vaste offerte di servizi online tocchino oramai tutti gli aspetti della vita sociale (si pensi *all'e-government, all'e-commerce,* o proprio *all'e-health*), figurandosi quale terreno fertile di recenti scorribande poste in essere da gang di cyber-criminali, contraddistinte dal raffinato *know-how* tecnologico: la minaccia, la compromissione ed il danneggiamento dei sistemi informatici, così come la sottrazione illecita di dati ed informazioni ivi contenute al fine di ricavarne un immediato profitto, o di utilizzarli indebitamente per ulteriori scopi

---

102 A. Apruzzese, "Autori e vittime nella criminalità informatica", in *Rivista di Criminologia, Vittimologia e Sicurezza,* Vol. III, n. 3 - Vol. IV, n. 1, Settembre 2009 - Aprile 2010, pp. 101-106.

103 Intendendosi quei soggetti ben lontani dai principi e dagli ideali della cosiddetta "etica hacker", ossia coloro che operano *system-cracking* al puro scopo di violare i sistemi informatici, per acquisire informazioni riservate o anche per puro vandalismo.

illeciti, rappresentano difatti le condotte che maggiormente infondono una sensazione di insicurezza generale, esponendo al pericolo la prosperità del sistema sociale nel suo complesso.[104]

Peraltro la suddetta rinnovata criminalità informatica si presenta proprio con le tipiche caratteristiche di impresa, andando a gestire in forme tutt'affatto che innovative, il business del malaffare informatico: boss, ossia raffinate menti con spiccate capacità manageriali, individuano, arruolano ed ingaggiano abilmente ed in varia forma,[105] facendoli ruotare attorno a sé, sia tecnici esperti (ad esempio nell'allestimento di siti clone, nell'utilizzo di *botnet*,[106] od ancora nella creazione e diffusione di *malware*), sia stuoli di gregari con mansioni meramente esecutive, destinati cioè alle attività di monetizzazione degli ingenti proventi derivanti dalle ruberie informatiche.

Allora si capirà come da un lato i vecchi *cracker* non appaiano più come i principali ed autonomi autori dei crimini informatici, ma piuttosto quali meri prestatori d'opera (a volte stabilmente inseriti nelle imprese criminali, altre volte ingaggiati all'occasione), dall'altro lato come affiorino poi nuove figure, centinaia di "soldatini" inseriti in nuovi schemi di riciclaggio, che si prendono cioè carico di ricevere le somme truffate, di rigirale ad altri sconosciuti "commilitoni", andando ad avviare così un tortuoso iter di "lavaggio" del denaro sporco, che renderà particolarmente arduo il risalimento ai reali beneficiari.[107]

È quindi di questo che si tratta: abili "burattinai" che muovono al meglio le pro-

---

104 D. Vulpiani, "La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto", in *Rivista di Criminologia, Vittimologia e Sicurezza,* Vol. 1, n.1, Gennaio - Aprile 2007, pp.1-9.

105 Sotto questo profilo la stessa "Rete delle reti" Internet presenta notevoli potenzialità relazionali, basti pensare alle stanze di chat, ai forum, come anche alle reti di social network quali pratici mezzi per selezionare e reclutare i migliori esperti di informatica, o altresì per entrare in disponibilità dei virus più raffinati.

106 Il termine, crasi dei due vocaboli inglesi *robot* e *network*, sta ad indicare un insieme di programmi informatici che eseguono in maniera automatica e ripetitiva operazioni che altrimenti richiederebbero l'intervento di un operatore "umano" alla tastiera. Tali programmi possono essere utilizzati per acquisire il controllo remoto di interi gruppi di computer e far compiere a tali macchine, ormai fuori dal controllo degli effettivi titoli, operazioni indesiderate, prevalentemente per fini illeciti (si pensi ad attacchi ad interi sistemi informatici, *spamming*, o ancora a furti di dati identificativi personali).

107 A. Apruzzese, "Dal computer crime al computer-related crime", in *Rivista di Criminologia, Vittimologia e Sicurezza,* Vol. I, n.1, Gennaio 2007 pp. 1-6.

prie schiere di “marionette” (quali tecnici informatici, riciclatori e gregari vari), seguendo svariati disegni criminali, che siano orientati all’esclusivo e ben noto scopo dell’illecito arricchimento.

Seppur ricondotte nell’alveo criminologico classico delle attività finalizzate al mero scopo di lucro, le sopradette nuove devianze presentano tuttavia alcune particolari connotazioni: *in primis* il singolare rapporto tra boss e gregari, molto spesso infatti questi ultimi non hanno mai veramente l’occasione di conoscere i primi, *in secundis* innovativo risulta essere altresì il rapporto autore-vittima, appare infatti allontanarsi sempre più il diretto contatto tra criminale-aggressore e vittima del raggiro. Per chiarire tale ultimo aspetto si pensi all’evoluzione del fenomeno del phishing: da forma frodatoria in cui la “leggerezza” della vittima giocava un ruolo cardine nell’agevolare la conclusione dell’iter truffaldino si sta progressivamente transitando verso nuove modalità di infezioni informatiche (si pensi al *keylogging*) in cui *l’identity theft* prescinde del tutto da atteggiamenti “colpevolmente negligenti” del derubato, essendo in sostanza vittima diretta dell’inganno solamente più lo stesso elaboratore elettronico, nella anzi più totale inconsapevolezza degli stessi utilizzatori.[108]

È indubbio che per contrastare efficacemente tali forme criminali servirà da una parte individuare un equilibrato punto di fusione tra competenze tecnico-informatiche e capacità investigative classiche, d’altra parte si paleserà sempre più imprescindibile una risposta su ampia scala, orchestrata cioè tra forze di polizia ben collegate e coordinate in ambito internazionale. Ovvio è infatti che tali nuove imprese criminali non conoscano barriere territoriali, ogni concetto di territorialità invero si dissolve proprio in ragione della dimensione mondiale del fenomeno e della natura stessa del mezzo utilizzato (ossia Internet e le reti telematiche in generale), per questa ragione risulta oltremodo essenziale e doverosa una stretta e concreta sinergia fra omologhe strutture investigative operanti in differenti contesti nazionali.

Chiaro è che i nuovi fenomeni criminali che minacciano la popolazione internauta, nonché le stesse infrastrutture tecnologiche siano della natura più svariata:

---

108 *Ibidem*.

truffe via internet, clonazioni di carte di pagamento, azioni di *hacking*, pedopornografia online, diffusione di codici malevoli, *spamming*, *phishing*, o altresì diffusione di opere dell'ingegno in violazione dei diritti d'autore.

Ciononostante cercando di accostarsi al nodo centrale della qui presente trattazione, si vorrà, più avanti, spostare l'attenzione verso l'analisi del modus operandi, nonché delle peculiarità tipiche delle cyber-gang criminali che ad oggi siano operative nello specifico settore *dell'health system.* Prima di fare questo si concluda il suddetto capitolo con qualche, doverosa, riflessione circa il venire alla luce di una nuova categorie di vittime: le cyber vittime.

3.6 Nuove vittime: le cyber-vittime

Più della metà della popolazione mondiale è online: un abitante su due del pianeta è a rischio di divenire vittima di criminalità online,[109] eppure si conosce davvero molto poco a proposito vittime di cybercriminalità, e questo perché le statistiche sul tema sono piuttosto rare.

In piena società digitale possiamo così affermare quanto non si siano sviluppati ancora, come è accaduto invece per altre forme di vittimizzazione, questionari standard, con domande al passo coi tempi, calibrate e ritagliate *ad hoc* rispetto alla cyber-criminalità, inoltre non esistono esperienze di indagini di vittimizzazione sulla cybercriminalità comparate a livello sovranazionale, ed ancora le indagini esistenti riguardano principalmente individui e non aziende, nonostante anch'esse risultino in egual misura nel mirino di svariati attacchi informatici.[110]

Allo stato dei fatti dunque continua ad avere ragione Wall, il quale ritiene esserci larga confusione su chi siano le vittime del crimine informatico e su come venga-

---

109 C.M.M Reep-van den Bergh, M. Junger, "Crime science", in *Victims of cybercrime in Europe: a review of victim surveys,* 7(5), 2018, pp. 1-15

110 A. Di Nicola, op. cit. *supra* a nota 58, p. 77

no queste stesse vittimizzate: il problema alla base di tale confusione è che molte vittime di crimini informatici non vogliono riconoscere di esser state vittime o potrebbero non rendersi effettivamente conto di esserlo state.

A tal proposito si possono richiamare le parole di Jaishankar: *"La maggior parte degli studiosi, escludendone pochi, ritiene che la cyber-vittimizzazione equivalga alla vittimizzazione da cyber-bullismo e da cyber-stalking. [...] Ma non includere altri tipi di criminalità informatica nella prospettiva della vittimizzazione non è corretto. [...] Inoltre ogni volta che viene analizzata la vittimizzazione informatica, viene esaminata solo da una prospettiva individuale e non da una prospettiva di massa o di sistema. Non solo gli individui possono essere vittime di criminalità informatica, ma anche i governi, le aziende e la società".* [111]

Così partendo dall'assunto che esistono diversi paradigmi interpretativi e svariati modelli teorici atti a decifrare i fenomeni della vittimizzazione ripetuta o della sua concentrazione spazio-temporale, si proverà ora a spiegare cosa potrebbe significare occuparsi di vittime nella società digitale.

Per far ciò si richiami qui brevemente il modello di Fattah, [112] tendente a raggruppare i fattori rilevanti del rischio di vittimizzazione in dieci categorie, quale teorizzazione applicabile e ripensabile alla luce dell'architettura propria di una società digitale:

a. Opportunità. Le caratteristiche dei target (persone, famiglie, imprese etc.) e delle loro attività definiscono la struttura delle opportunità con conseguenze sui rischi di vittimizzazione. Ed è proprio così che la società digitale arriva a modificare la struttura delle opportunità nel mondo sia fisico che virtuale: quali persone, quali famiglie, quali aziende e quanto, come, per quali attività usino Internet e come questo cambi i loro stili di vita può determinare occasioni per eventi criminali offline ed online.

---

111 K. Jaishankar, "Cyber victimology: a new sub-discipline of the twenty-first century victimology", in J. Joseph, S. Jergenson (a cura di) *An international perspective on contemporary developments in victimology,* Springer, Cham, 2020, pp. 3-19.

112 E.A. Fattah, "Victimology: past, present and future", in *Criminologie*, 33(1), 2020 pp. 17- 46.

b. Fattori di rischio altamente specifici. L'alfabetizzazione tecnologica o le competenze di *guardianship* di carattere tecnologico, collegate a caratteristiche socio-demografiche quali età, sesso, livello di reddito, trasformano senza dubbio i rischi di vittimizzazione per reati a basso ed alto contenuto tecnologico.

c. Reo motivato. I potenziali autori non scelgono i loro target casualmente ma in base ad una attenta ed accurata selezione alla luce di criteri specifici, ciò vale anche per i criminali tecnologici che scelgono difatti le potenziali vittime attraverso processi razionali e sempre più oggettivi. Oggi un cyber-criminale può sapere quanto un sistema informatico sia vulnerabile, quanti "buchi" presenti, oppure potrebbe servirsi di analisi avanzate di *Big Data* per identificare le sue vittime allo scopo di rendere più efficace e meno rischiosa la sua attività criminale.

d. Esposizione. L'esposizione a potenziali criminali e a situazioni o ambienti ad alto rischio accresce indubbiamente la vittimizzazione: così anche il tempo passato online può essere un fattore di rischio nuovo per i reati cibernetici, come anche per specifici reati offline.

e. Associazioni. Individui che sono in contatto personale, sociale o professionale con potenziali delinquenti hanno un rischio maggiore di subire reati. Al tempo di internet le nuove associazioni fra criminali e vittime possono essere virtuali, potendo passare reciprocamente molto tempo assieme ed instaurando anche forti relazioni sociali, senza incontrarsi mai fisicamente.

f. Spazi e tempi pericolosi. Il rischio di vittimizzazione non è equamente distribuito nello spazio e nel tempo. Ci si potrebbe domandare se rispetto ad una vittimizzazione digitale esistano tempi più pericolosi o luoghi digitali più imprudenti da frequentare e che rapporto vi sia fra luoghi e tempi offline ed online rispetto ai rischi stessi.

g. Comportamenti a rischio. Nel mondo fisico alcuni comportamenti possono accrescere il rischio di vittimizzazione, esistono infatti azioni che dispongono colui che le mette in atto in situazioni pericolose, riducendo notevolmente la capacità di difendersi. Ciò si può traslare agilmente sul piano digitale: si pensi al lasciare informazioni personali sui social media, prassi con cui ci si sottopone al rischio di divenire vittima di alcuni reati fisici, quali i furti di identità.

h. Attività ad alto rischio. Il coinvolgimento in attività ad alto rischio può accrescere i livelli di vittimizzazione. Se nel mondo fisico ciò può accadere nel compiere attività ricreative o di ricerca di divertimento, nel mondo digitale questi concetti potrebbero dover in parte esser rimodellati.

i. Comportamenti di difesa. Una larga parte della vittimizzazione può essere evitata efficacemente tramite attitudini e comportamenti difensivi. Allora ci si può chiedere quali siano i nuovi comportamenti di difesa da mettere in campo online e offline e come possano questi rappresentare estensioni dei comportamenti di difesa abituali.

j. Propensione strutturale/culturale. La povertà, la marginalità, la deprivazione sono correlate positivamente a certi tipi di vittimizzazione. Ci si chiede allora se ciò abbia un qualche valore anche nel mondo delle tecnologie, se cioè determinati processi di marginalizzazione e stigmatizzazione possano nascere anche nel mondo online.

Risulta ormai, a questo punto della trattazione, chiaro come gli effetti della digitalizzazione della società si esplichino anche sul versante delle vittime della criminalità e sugli stessi processi di vittimizzazione: alla criminologia allora, e più specificatamente alla vittimologia, non resta che prenderne atto e provare a muoversi abilmente di conseguenza.

CAPITOLO 4

SANITÀ SOTTO ATTACCO

4.1 Report: un settore altamente vulnerabile

Con le seguenti allarmanti parole si avvia la prefazione del tradizionale rapporto CLUSIT 2020 sulla sicurezza ICT [113] in Italia: *"Nell'anno appena passato si è consolidata una discontinuità, si è oltrepassato un punto di non ritorno, tale per cui ormai ci troviamo a vivere ed operare in una dimensione differente, in una nuova epoca, in un altro mondo, del quale ancora non conosciamo bene la geografia, gli abitanti, le regole e le minacce"*. La convinzione, prosegue il Rapporto, è che sia avvenuto *"un vero e proprio cambiamento epocale nei livelli di cyber-insicurezza, causato dall'evoluzione rapidissima degli attori, delle modalità, della pervasività e dell'efficacia degli attacchi"*. [114]

Il quadro così delineato dal rapporto Clusit va a destrutturare quella convinzione di cybersecurity fin troppo spesso associata a "realtà suggestive" (o fantascientifiche), distanti dalla vita di tutti i giorni, nonché appannaggio dei soli protagonisti della governance statale ed internazionale.

In una comunicazione congiunta, del 13 Settembre 2017, al Parlamento Europeo e al Consiglio traspare, con nitidezza, come i rischi cibernetici stiano aumentando in maniera esponenziale: *"Secondo alcuni studi l'impatto economico della cybercriminalità è aumentato di cinque volte tra il 2013 e il 2017 e potrebbe ancora quadruplicarsi entro il 2019. [...] Se non miglioreremo sostanzialmente la nostra cybersicurezza il rischio aumenterà in funzione della trasformazione digitale."* Dunque è senza dubbio diventato fondamentale rafforzare una cyber-resilienza attraverso *"un solido mercato unico, importanti progressi nella capacità tecnologica nell'Unione e un numero molto più elevato di esperti qualificati"*. [115]

---

113 Per ICT (acronimo di *Information ad Communications Technology*) si intendono tutti i processi e le pratiche connesse alla trasmissione, ricezione ed elaborazione dei dati e delle informazioni.

114 Per una sua approfondita analisi si rimanda al *Rapporto Clusit 2020 sulla sicurezza ICT* in Italia reperibile al sito internet https://clusit.it/

115 Commissione Europa, Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, *Comunicazione congiunta al Parlamento e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, Bruxelles, 13 Settembre 2017, reperibile al sito internet https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX%3A52017JC0450

Allora il fine che si è indirizzati a perseguire è proprio una accettazione più ampia del fatto che la cybersicurezza rappresenti una sfida sociale comune, motivo per cui dovrebbero essere coinvolti, in ottica di risposta, molteplici livelli: dell'amministrazione pubblica, dell'economia e della società.

Ovvio è come, in tale contesto, alcuni ambiti specifici debbano affrontare altrettanto specifiche problematiche, che impongono una integrazione delle strategie di cybersecurity di carattere generale con quelle di tipo settoriale: ed uno dei settori specifici che, negli ultimi decenni, più di altri ha subito notevoli trasformazioni, con un progressivo utilizzo di nuove tecnologie è proprio quello sanitario.

Il mercato sanitario invero si figura sempre più attenzionato da parte dei c.d. Tech Giants (Google, Amazon, Walmart etc.), i quali promettono di rivoluzionarne le tradizionali modalità di assistenza sanitaria attraverso una digitalizzazione dei servizi e una disintermediazione degli stessi rispetto agli erogatori tradizionali.

Il settore sanitario è presto diventato così un banco di prova paradigmatico per nuove ed ardue questioni, poste innanzitutto ai giuristi, in ragione specialmente della straordinaria mole di dati accumulati, della articolata complessità dei rapporti giuridici che vi si instaurano, nonché della esigenza di garantire il più alto livello possibile di sicurezza e privacy.[116]

Prima di procedere alla disamina delle principali condotte di cyber-criminalità che colpiscono *l'healthcare system,* si vuole qui fornire una panoramica sulla gravità e pericolosità degli attacchi, in quanto impattanti su un settore altamente vulnerabile: come si può intuire infatti c'è un legame diretto tra gli attacchi informatici subiti dalle strutture sanitarie e le condizioni dei pazienti che si affidano alle loro cure.

A tal fine si richiama il recente report condotto da Ponemon Institute, una delle principali organizzazioni di ricerca sulla sicurezza informatica, in unione con Pro-

---

116 E. Macrì, "Il quadro giuridico del cyber risk", in *Capire il rischio cyber: il nuovo orizzonte in sanità*, white-paper SHAM Italia, 2021, pp. 15 - 22.

ofpoint, società leader nel settore della cybersecurity e compliance, dal titolo *"Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care"*. [117]

Lo studio vede coinvolti 641 professionisti dell'It *(Information technology)* quali responsabili, nonché partecipanti all'elaborazione di strategie di sicurezza informatica sanitaria, e fin da subito pone in marcata evidenza come l'89% delle organizzazioni intervistate dichiari di aver subito una media di 43 attacchi negli ultimi 12 mesi, quasi uno a settimana.

Si continua poi andando a delineare i quattro tipi di attacchi più comuni: la compromissione del cloud, l'attacco ransomware, alla supply chain, [118] ancora la compromissione delle e-mail aziendali/spoofing [119] ed il phishing. [120]

Ecco che tali attacchi vengono messi in relazione con le loro dirette conseguenze verificatesi in sanità: da ritardi nelle procedure e negli esami, alla degenza più lunga dei pazienti, ad un loro progressivo trasferimento in altre strutture sanitarie, al sorgere di maggiori complicazioni nel fornire prestazioni sanitarie, fino ad un incremento dei tassi di mortalità. [121]

Così difatti recita il quesito formulato nel report, con l'ovvia possibilità per gli intervistati di apporre più di una risposta: *"Se la tua organizzazione ha subito queste tipologie di attacchi informatici, quale impatto hanno avuto sulla cura dei pazienti?"*.

---

117 Ponemon *Institute, Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care,* 2022, reperibile al sito internet https://www.proofpoint.com/us/cyber-insecurity-in-healthcare.

118 Un attacco alla supply chain (chiamato anche attacco di terze parti) avviene quando l'aggressore accede alla rete di un'azienda tramite una terza parte fornitrice. Questo tipo di attacco necessita di un software o di una singola applicazione compromessa per diffondere il malware nell'intera catena di fornitura. Di solito prende di mira il codice sorgente di un'applicazione, inserendo così il proprio codice dannoso nel sistema.

119 Per spoofing ci si riferisce all'impersonificazione da parte di un hacker di un altro dispositivo o di un altro utente su una rete al fine di impadronirsi di dati, diffondere malware o superare dei controlli di accesso.

120 Per phishing si intende quel tipo di attacco che consiste nell'inviare e-mail malevoli scritte appositamente con lo scopo di spingere le vittime a cadere nella trappola dei cybercriminali. Spesso lo scopo infatti è di portare gli utenti a rivelare informazioni bancarie, credenziali di accesso o altri dati sensibili.

121 Ponemon Institute, op. citata supra a nota 117, p. 11

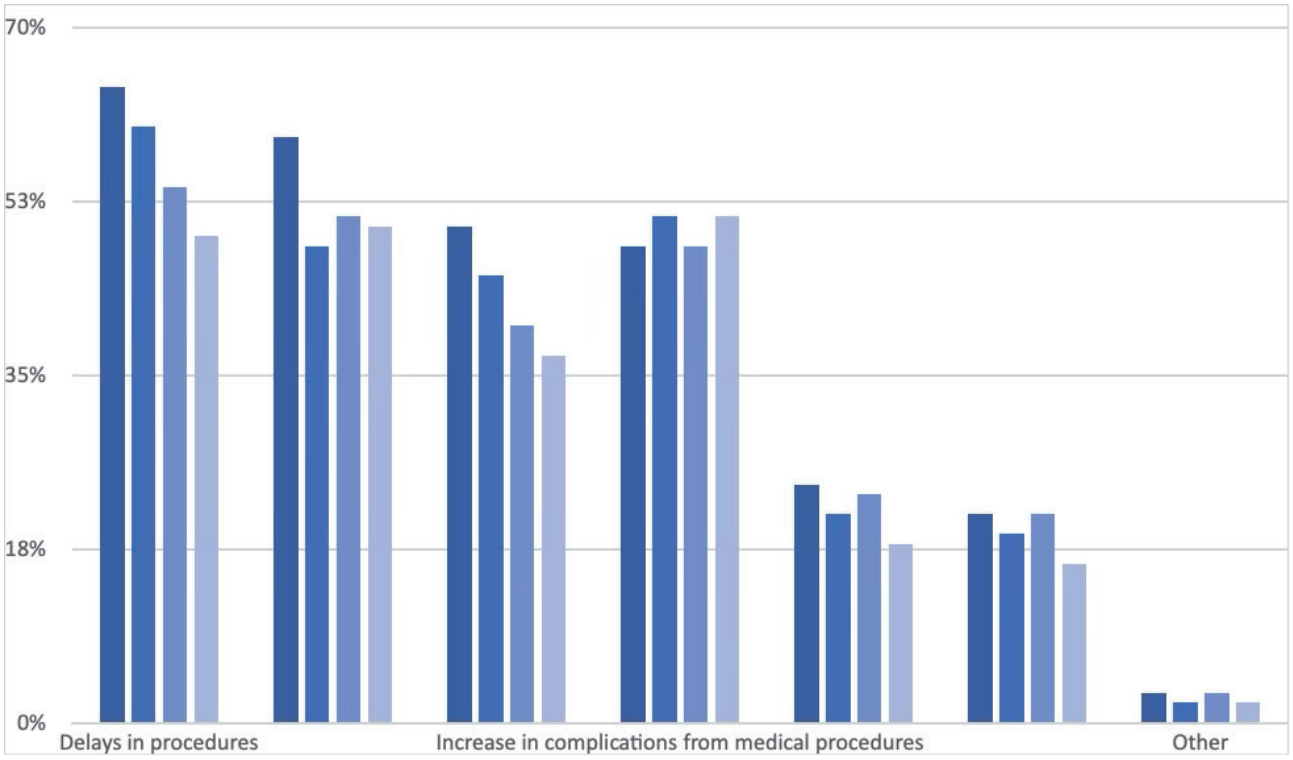

Fig. 4.1 Elaborazione dati Ponemon Report: cyberattacchi - conseguenze sanitarie.

Si è voluto innanzi graficamente rappresentare i dati raccolti *(Figura 4.1)* al fine di poter constatare come l'attacco ransomware rimanga a tutti gli effetti una sfida significativa: è difatti la tipologia di attacco informatico con la maggiore probabilità di influire sulla cura dei pazienti rispetto alle altre tipologie malevoli (il 64% delle aziende colpite da ransomware ha registrato ritardi nelle procedure mediche e quasi altrettante hanno visto prolungare le degenze dei pazienti).

Tali risultati rimarcano come le organizzazioni sanitarie dovrebbero dare maggiore priorità alla sicurezza IT, in questo senso commenta Larry Ponemon, presidente e fondatore di Ponemon Institute: *"Gli attacchi che abbiamo analizzato mettono a dura prova le risorse delle organizzazioni sanitarie. Il risultato non è solo una enorme perdita economica, ma anche un impatto diretto sull'assistenza ai pazienti, che mette in allarmante pericolo la loro sicurezza e salute"*.

A seguire si riportano altri risultati chiave emersi dal report:[122]

122 Ponemon Institute, op. citata *supra* a nota 93, p. 5

a. Dispositivi medici e mobile apps rimangono una delle principali preoccupazioni in tema di cybersicurezza. A tal proposito si usa l'espressione di *Internet of Medical Things* (IoMT) per indicare tutti i devices medici, di varia natura, collegati ad una struttura o ad un operatore sanitario tramite internet, in grado di generare, raccogliere, analizzare e trasmettere dati sanitari (si pensi a dispositivi indossabili, strumenti per il monitoraggio remoto dei pazienti, pompe di infusione, pacemakers). Le organizzazioni sanitarie hanno in media più di 26.000 dispositivi connessi alla rete: sebbene il 64% degli intervistati si sia dichiarato preoccupato per la sicurezza inerente a tali devices medici, solamente il 51% di questi afferma che la propria organizzazione si sia effettivamente provvista di strategie di sicurezza informatica di prevenzione e risposta a possibili attacchi contro tali dispositivi.

b. Le organizzazioni si sentono al contempo più vulnerabili e più preparate alla compromissione del cloud: il 75% degli intervistati si dichiara difatti vulnerabile verso tali tipologie di attacchi e il 54% afferma di averne subito almeno uno negli ultimi due anni (le organizzazioni ricomprese in quest'ultimo gruppo arrivano a sostenere una media di 22 compromissioni negli ultimi due anni). Tuttavia, oltre ad essere più vulnerabili, si dichiarano anche maggiormente preparate ad affrontare tali minacce, con il 63% che dichiara di aver optato per l'adozione di misure specifiche al fine di esser preparati nel rispondere a simili cyberattacchi.

c. Il ransomware è la seconda più sentita vulnerabilità con il 72% degli intervistati che ritiene la propria organizzazione esposta a tale cyber-rischio, e con il 60% che sostiene come sia effettivamente la tipologia di attracco che desta maggiori preoccupazioni. Negli ultimi due anni le organizzazioni che sono state sottoposte ad attacchi ransomware (41% degli intervistati), hanno subito una media di tre di questi attacchi.

d. La mancanza di preparazione mette a rischio tanto le organizzazioni sanitarie quanto i pazienti stessi. Meno della metà degli intervistati dichiara di avere effettivamente una strategia documentata da seguire per gli attacchi spoofing/phishing (48%), e ugualmente per gli attacchi alla supply chain (44%).

e. I programmi di formazione e sensibilizzazione al cyber-rischio, insieme al monitoraggio dei dipendenti, rappresentano una delle principali strategie per mitigare le minacce informatiche: solo però il 59% degli intervistati ha dichiarato che la propria organizzazione stia affrontando concretamente il problema della mancanza di cyber-consapevolezza tramite o l'adozione di programmi di *training* per i dipendenti o monitorando il loro stesso operato.

f. La mancanza di competenze interne, fondi e risorse mettono anch'essi a dura prova la sicurezza informatica complessiva: il 53% degli intervistati sostiene di soffrire la mancanza di competenze interne specializzate e il 46% afferma come il personale lavorativo risulti insufficiente.

g. I cyberattacchi provocano enormi costi. È stato chiesto agli intervistati di stimare il singolo attacco informatico più dannoso subito negli ultimi 12 mesi: sulla base delle risposte ottenute, il costo totale medio per l'attacco informatico più dannoso è stato di 4.4 milioni di dollari, con una perdita di produttività quale conseguenza finanziaria di circa 1.1 milioni di dollari.

Da tale studio si è ricavata l'urgente necessità di investire nella cyber security: si è visto chiaramente come una scarsa protezione IT possa avere effetti assolutamente profondi e tangibili tanto sulla struttura sanitaria quanto sui pazienti. Purtroppo ancora oggi gli investimenti in termini di sicurezza vengono visti unicamente come costi e per questo spesso limitati il più possibile; se invece ci si rendesse conto che si tratta di veri e propri investimenti dotati di un loro ritorno

in diminuzione dei rischi, molti incidenti potrebbero essere fortemente limitati se non evitati, assieme ad un ingente risparmio sia di tempo che di denaro. [123]

Così conclude commentando Ryan Witt, *healthcare cybersecurity* leader di Proofpoint: *"L'assistenza sanitaria è rimasta indietro rispetto ad altri settori nell'affrontare il crescente numero di attacchi informatici, e questa immobilità impatta negativamente sulla sicurezza e sul benessere dei pazienti. [...] Finché la sicurezza informatica rimarrà una priorità di basso livello, gli operatori sanitari continueranno a mettere in pericolo i loro stessi pazienti. Per evitare conseguenze drammatiche, le organizzazioni sanitarie devono allora comprendere come la cybersecurity influisca sull'assistenza ai pazienti e mettere in atto i passi necessari per proteggere al meglio le persone e i loro dati"*.

Ed è proprio di dati che nel diretto prosieguo si tratterà, o meglio, delle loro sempre più frequenti illecite violazioni, divulgazioni, perdite e compromissioni, anche conosciute col nome di *Data breaches*.

123 A. Gelpi, "La Sicurezza dei dati sanitari", in Torino Medica. La rivista dell'ordine dei medici chirurghi e odontoiatri della provincia di Torino, anno XXXIII, numero 3-4, 2021, pp. 11-21.

A. DATA BREACH

4.2 Nuova frontiera della privacy: la protezione dei dati personali

La nozione di privacy trova una sua primordiale accezione nel *"right to be alone"* [124] teorizzato dai due giuristi statunitensi Warrein e Brandeis nel 1890, traducendosi nel diritto dei singoli alla riservatezza: uno spazio della vita, quasi fisico, da cui il soggetto aveva diritto di tenere esclusi gli altri, a loro volta doverosi di rispettarne l'individualità, una sorta di *"tutela dell'intimità privata"*. [125]

Sin da subito si può constatare come esso si presenti quale diritto a contenuto essenzialmente negativo, comprendente il non subire ingerenze, il non far conoscere e il mantenere riservate alcune informazioni, piuttosto che a contenuto positivo, che viceversa si avrebbe con l'esercitare un effettivo controllo sulle informazioni medesime.

La definizione di privacy innanzi prospettata appare però, oramai da qualche decennio, non più perfettamente corrispondente alle trasformazioni socio-economiche subite dalla società, soprattutto alla luce della sua preponderante digitalizzazione. Per chiarire, con l'avvento della stagione degli elaboratori elettronici e con l'introduzione della ragnatela del web, la circolazione dei dati personali è divenuta indubbiamente regola fisiologica della società: una società per l'appunto denominata "dell'informazione e della comunicazione".

Ecco che allora la diffusione e l'utilizzo delle nuove tecnologie e delle reti informatiche hanno prodotto un mutamento semantico del concetto di tutela della privacy: nata come diritto dell'individuo borghese a escludere gli altri da ogni forma di invasione della propria sfera privata *("my home, my castle")*, si è sempre

---

124 S. Warren, L.D. Brandeis, "The right to Privacy", in *Harvard Law Review,* Vol. 4, No. 5, 1890, pp.193-220.

125 P. Rescigno, *Diritti della personalità,* Enc. Giur. Treccani, Roma, 1994.

più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi su trovino, riflettendo così il nuovo contesto in cui ogni persona cede continuamente e nelle forme più diverse dati che la riguardano. [126]

Di qui alcuni studiosi sono arrivati a formulare il cosiddetto *"privacy paradox"*: [127] le condotte di condivisione di informazioni (si pensi all'uso dei *social networks*) non sempre implicano anche la consapevolezza da parte degli utenti della divulgazione che i propri dati possono avere. A tal proposito asserisce Antonello Soro, Presidente dell'autorità Garante per la protezione dei dati personali: *"Poiché i dati rappresentano la proiezione digitale delle nostre persone, aumenta in modo esponenziale anche la nostra vulnerabilità. La libertà di ciascuno è insidiata da forme sottili e pervasive di controllo, che noi stessi, più o meno consapevolmente, alimentiamo per l'incontenibile desiderio di continua connessione e condivisione"*. [128]

D'altronde mentre la violazione di altri diritti fondamentali quali libertà personale, integrità personale, libertà di parola, si risolve più frequentemente in fatti e comportamenti visibili, spesso la violazione del diritto alla riservatezza si risolve in fatti e comportamenti di più difficile percezione, ma ugualmente di estrema gravità. E tale percettibilità delle violazioni è ancora minore in Internet rispetto alla vita reale. Per esser chiari, si voglia fornire un' esemplificazione.

Se ad un individuo che entrasse in un negozio fosse sfilato il portadocumenti al fine di copiare l'indirizzo di casa e spedire continuamente materiale pubblicitario mirato, o per controllare le ricevute della carta di credito dalle quali ricavare ciò che l'individuo ha comprato nelle settimane precedenti, o ancora per ricavare dalle diverse tessere di cui è in possesso il suo orientamento politico, sindacale ed i suoi interessi sociali, tale soggetto si sentirebbe di certo profondamente leso dall'aver subito grave abuso.

---

126 S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza-la Repubblica, Roma-Bari, 2014, pp. 27-32

127 S.B. Barnes, "A privacy paradox: Social networking in the United States", in *First Monday*, Issue 11/9, 2006.

128 Intervento di A. Soro, Presidente dell'autorità Garante per la protezione dei dati personali, Big Data: *La nuova geografia dei poteri,* in occasione della Giornata Europea della protezione dei dati personali, 30 Gennaio 2017.

Questo ed altro avviene in rete, e non vi è reazione lontanamente avvicinabile. [129]

Ora, tornando all'evolvere del concetto di privacy, a fronte quindi di un individuo messo a nudo, nella sua intimità, da una tecnologia sempre più invasiva (che è legata al polso da un orologio smart, che entra nelle case con una televisione di ultima generazione, che segue gli spostamenti in auto attraverso l'utilizzo di sensori connessi ad internet), la privacy segue un mutamento di rotta, finendo per essere ridefinita nella più comprensiva nozione di "protezione dei dati", concetto che va ben oltre ai problemi legati alla difesa della sfera privata, abbracciando regole generali sulla circolazione delle informazioni. [130]

Il diritto alla protezione dei dati personali può essere definito come il diritto a che le informazioni su una persona fisica individuata o individuabile siano raccolte e trattate in modo lecito: esso consiste dunque nel diritto del soggetto cui i dati si riferiscono di esercitare un controllo, anche attivo, su detti dati, che si estende dall'accesso alla loro rettifica. [131]

Si qualifica allora come un diritto proprio di ogni soggetto ad autodefinirsi e determinarsi, dal contenuto fortemente positivo, consistente nell'esercitare un controllo effettivo sul flusso delle proprie informazioni, distinguendosi dalla mera riservatezza quale libertà negativa di non subire interferenze.

Con l'entrata in vigore del GDPR, e la consequenziale modifica al Codice della Privacy intervenuta con d.lgs. 10 Agosto 2018, n. 101, ha trovato allora finalmente realizzazione nell'ordinamento italiano quel microsistema autonomo basato sul riconoscimento di un nuovo bene giuridico di settore: il trattamento dei dati personali, su cui peraltro svariati cenni sono già stati fatti nel discorrere del secondo capitolo, a cui si rimanda.

Si consideri comunque che la stessa giurisprudenza europea condivideva il biso-

---

129 Per un dettagliato approfondimento sul tema si rimanda a N. Lugaresi, *Internet, privacy e i pubblici poteri negli Stati Uniti,* Giuffrè editore, Milano, 2000.

130 F. Carlino, "L'origine della privacy e l'esigenza di tutelare i dati personali", in *Iusinitinere*, Rivista Semestrale di diritto, ISSN 2724-2862, 4 Luglio 2020, aggiornato 13 Luglio 2020, pp. 1-13.

131 G. Finocchiaro, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli editore, Bologna, 2017, p. 6.

gno di mutare l'approccio consolidatosi negli anni precedenti, basato su di una statica tutela della riservatezza. La Corte di Lussemburgo, infatti, aveva più volte evocato il concetto di "sovranità digitale", allo scopo di indurre i legislatori nazionali a prendere in debita ed attenta considerazione l'esistenza di un nuovo ordinamento giuridico, l'ordinamento digitale, inteso come spazio immateriale in cui confluiscono e vengono trattati dati personali digitali.

Architravi della nuova disciplina risultano essere i fondamentali principi del consenso e di *accountability* che, si voglia ripetere anche in questa sede, consiste nella responsabilizzazione di chi è titolato a trattare i dati, cui viene imposta, tramite l'ordine di rendicontazione, una gestione idonea a garantire la piena conformità del trattamento ai principi sanciti dal Regolamento Ue e dalla legislazione interna. [132]

Pare, tuttavia, che l'evoluzione legislativa si sia qualitativamente arrestata, nonostante i proclami in materia di prossime regolamentazioni [133] e nonostante l'approvazione del GDPR: il diritto alla protezione dei dati personali, per come oggi regolamentato, si appalesa anacronistico. Rimane infatti un diritto che affonda le proprie radici nella società degli anni Settanta, che si apprestava a diventare la Società dell'informazione, un mondo ad oggi profondamente mutato: il dato è sempre meno controllabile, fra *Big Data* [134] e sistemi in *cloud*, o comunque sostanzialmente inaccessibile a chi dovrebbe sorvegliare l'applicazione della normativa.

Se da un lato le tecnologie che plasmano la società avanzano ad un ritmo impressionante, dall'altro gli strumenti di protezione effettiva diventano sempre più obsoleti, senza tuttavia essere aggiornati o rimpiazzati, il che causerà conseguenze particolarmente gravi nei settori a maggior rischio, come quello della salute. [135]

---

132 G. Fornari, *Il trattamento dei dati: rischi penali e compliance dell'impresa,* Fornari e Associati studio legale, Milano-Roma, Gennaio 2021, p 2-4.

133 Si pensi, in particolare, alla proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale, del 21 Aprile 2021.

134 Con tale locuzione si indica una ingente mole di dati informatici, le cui caratteristiche sono facilmente riassumibili seguendo il modello delle tre "V": Volume (grande quantità), Velocità (di generazione dei dati e della loro elaborazione) e Varietà (forte eterogeneità).

135 G. Fioriglio, "La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici", in *Journal of Ethics and Legal Technologies*, Volume 3(2), Novembre 2021, pp. 85-86.

Ai fini della trattazione, ciò che è fin qui stato detto nel discorrere di privacy dovrà essere necessariamente trasposto sul piano della sanità, per qualche considerazione.

Ormai è chiara l'evoluzione dal materiale al digitale che negli ultimi anni ha profondamente toccato il sistema sanitario italiano, evoluzione da cui emergono nuovi profili critici non soltanto per quanto riguarda l'efficienza delle cure e l'efficientamento delle strutture sanitarie, ma anche, e soprattutto, per quanto riguarda il coordinamento tra il diritto alla salute e il diritto alla protezione dei dati sanitari dei pazienti.

La nostra Carta Costituzionale all'art. 32 riconosce e tutela il diritto alla salute come diritto fondamentale dell'individuo e interesse della collettività, [136] prescrivendo altresì una riserva di legge rafforzata in forza della quale un trattamento sanitario previsto per legge *"non può in nessun caso violare i limiti imposti dal rispetto della persona umana"*. Formula questa complementare alla tutela della dignità, riconducibile all'art. 2 della Costituzione stessa. [137]

A sua volta, il diritto alla protezione dei dati, trova suo massimo riconoscimento nel secondo articolo costituzionale, in quanto riconducibile anch'esso all'esigenza di assicurare la dignità dell'interessato, che potrebbe essere difatti violata ogni qualvolta si verifichi un qualsivoglia *vulnus* nelle misure tecniche ed organizzative preposte alla tutela di tali dati. [138]

Entrambi i principi, tutela della salute e protezione dei dati personali, saranno allora meritevoli di una tutela intensa quanto dinamica, in costante adeguamento con l'evoluzione tecnologica e il progresso scientifico: sarà compito del giurista trovare il giusto equilibrio fra efficienza del sistema sanitario e delle cure e rischi per la dignità dei pazienti, derivanti dalla digitalizzazione dei dati sanitari.

---

136 *"La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti. Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana".*

137 *"La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale".*

138 F. Carlino, "il trattamento dei dati sanitari mediante il dossier sanitario", in *Iusinitinere*, Rivista Semestrale di diritto, ISSN 2724-2862, 29 Maggio 2020, pp. 1-3.

Ovvio è infatti come i dati sanitari, se illecitamente trattati, siano suscettibili di esporre l'interessato a forme di discriminazioni rese per l'appunto possibili dalla conoscenza di aspetti particolarmente intimi della persona, quali quelli idonei a rivelarne lo stato di salute.

Ad enucleare le criticità di una sanità digitale si richiamino, ancora una volta, le parole di Soro: *"Sotto questo profilo la strada da fare è ancora tanta: recenti ricerche hanno indicato, infatti, il settore sanitario come uno di quelli esposti ai maggiori rischi in termini di cyberattacchi perché carente di un piano organico di sicurezza e protezione, oltre che di risorse necessarie per investimenti sulle infrastrutture informative. Eppure proprio questo dovrebbe essere, invece, il settore su cui investire di più in termini di sicurezza informatica e digitale, per garantire che il processo di innovazione tecnologica sia accompagnato da misure tali da assicurare autenticazione dei dati, loro tracciabilità, accessi selettivi con credenziali univoche, cifrature, sistemi di alert, attività di auditing [...] La protezione del paziente da queste vecchie e nuove vulnerabilità deve essere un obiettivo centrale per un sistema sanitario all'altezza delle sfide della società digitale, in cui parallelamente alle opportunità (di ricerca, di cura, di avanzamento delle diagnosi e delle terapie) crescono anche i rischi."*[139]

4.3 Nozione di Data Breach

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi (si pensi ad incendi od altre calamità).

Così per *data breach* (o violazione dei dati personali) si intende ex art. 4 n.12 GDPR *"una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la*

139 Intervento di A. Soro, Presidente del Garante per la protezione dei dati personali, al convegno "La smaterializzazione dei documenti e il suo impatto sul sistema salute", Roma 6 Maggio 2016.

distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Ecco che una violazione di tal genere non può che compromettere quella triade CIA *dell'Information Security* di cui già si trattava nel previo capitolo, sorretta dai pilastri della riservatezza, integrità e disponibilità.

Si vogliano qui fornire alcuni possibili esempi di condotte riconducibili a tale definizione:

a. L'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;

b. Il furto o la perdita di dispositivi informatici contenenti dati personali;

c. La deliberata alterazione di dati personali;

d. L'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware etc.;

e. La divulgazione non autorizzata di dati personali.

Nelle previsioni del Regolamento Ue 2016/679 viene disciplinato in dettaglio il procedimento che il titolare del trattamento[140] dovrà porre in essere nel caso in cui sia in atto una simil violazione dei dati personali.

Dall'art. 33 GDPR si ricava infatti che il titolare del trattamento (soggetto pubblico, impresa, associazione etc.) senza ingiustificato ritardo, e ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza, deve notificare la violazione dei dati personali all'autorità di controllo competente (si intenda ivi il Garante per la protezione dei dati personali), a meno che sia improbabile che la violazione stessa comporti un rischio per i diritti e le libertà delle persone fisiche. Qualora la

---

140 Ex art. 4 n.7 GDPR per titolare del trattamento di intende *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".*

notifica al Garante sia effettuata oltre il termine delle 72 ore, dovrà essere corredata dai motivi del suddetto ritardo.[141]

Da ciò si ricava come siano da notificare unicamente le violazioni di dati personali che possono avere effetti significativi sugli individui, causando danni fisici, materiali o immateriali (si pensi alla perdita del controllo sui propri dati personali, ad un danno reputazionale, una perdita finanziaria, il furto di identità, la discriminazione o il rischio frode).

Al terzo comma del medesimo articolo si specifica che tale notifica dovrà avere come contenuto minimo:

a. Una descrizione della natura della violazione dei dati personali che comprenda, ove possibile, le categorie e il numero approssimativo di persone interessate nonché le categorie e il numero approssimativo dei dati personali interessati;

b. Il nome e i riferimenti di contatto del responsabile della protezione dei dati (se designato dal titolare) o comunque di un referente competente a fornire ulteriori informazioni;

c. Una descrizione delle possibili conseguenze della violazione dei dati personali;

d. Una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi.

Si noti come il responsabile del trattamento[142] che viene a conoscenza di una eventuale violazione sarà tenuto ad informare tempestivamente il titolare di modo che quest'ultimo possa attivarsi di conseguenza.

---

141 A partire dal 1 Luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo online https://servizi.gpdp.it/databreach/s/

142 Ex art. 4 n.8 GDPR per responsabile del trattamento si intende *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".*

Inoltre, a prescindere dalla notifica al Garante, il titolare del trattamento documenta tutte le violazioni dei dati personali, comprese le circostanze ad esse relative, le conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente alla stessa autorità di controllo di effettuare eventuali verifiche sul rispetto della normativa.

All'art. 34 GDPR viene prevista poi una ulteriore importante incombenza, collegata alla precedente, e cioè la comunicazione della violazione dei dati personali a tutti gli interessati, ovvero alle persone fisiche cui si riferiscono i dati personali oggetto del trattamento. Difatti quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrà necessariamente comunicarla, con linguaggio semplice e chiaro, agli interessati, senza ingiustificato ritardo. [143]

A norma del terzo comma tuttavia tale comunicazione non risulta esser dovuta unicamente nei casi in cui:

a. Il titolare del trattamento abbia messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure siano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi (si pensi ai sistemi di cifratura);

b. Il titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c. Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso si proceda invece tramite una comunicazione pubblica o simile misura di analoga efficacia.

---

143 *L'European Data Protection Board* ha fissato dei parametri per la valutazione dei fattori che determinano il rischio per le libertà e i diritti degli interessati, tra cui rientrano: il tipo di "breach", ossia il tipo di violazione; la natura, numero e grado di sensibilità dei dati personali violati; la facilità di associare i dati violati alla persona fisica; la gravità delle conseguenze per gli interessati ed il numero degli interessati esposti al rischio.

Nel caso in cui poi il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, la stessa autorità Garante potrà richiedere, dopo aver valutato la probabilità che la violazione rappresenti un rischio elevato, che vi provveda.

Qualora sia rilevata una violazione delle disposizioni del Regolamento Ue, il Garante potrà, ex art. 58 GDPR, prescrivere diverse misure correttive, fra le quali:

a. Rivolgere ammonimenti ed avvertimenti al titolare o al responsabile del trattamento;

b. Ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti stessi alle disposizioni del Regolamento, in una determinata maniera ed entro un determinato termine;

c. Ingiungere al titolare del trattamento di comunicare all'interessato la violazione dei dati personali;

d. Imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento, nonché ordinare la rettifica o la cancellazione di dati personali;

e. Infliggere una sanzione amministrativa pecuniaria ai sensi dell'art. 83 GDPR, in aggiunta alle misure correttive sopradette, o in luogo di tali misure.

Si ricavi come, quando si parla di violazioni della normativa in materia di privacy, il GDPR disciplini esclusivamente le sanzioni amministrative: il regolamento europeo stabilisce infatti, all'art. 84, che spetti a ciascuno Stato membro fissare autonomamente le sanzioni penali, purché queste ultime siano effettive, proporzionate e dissuasive.

Nel nostro ordinamento, come si avrà modo di approfondire in seguito, si è scelto dunque di mantenere in vigore quanto stabilito dal Codice della Privacy, emanato nel 2003, ed in particolare dagli articoli 167 e successivi, così come riformati dal d.lgs. n.101/2018.

Come sottolineato poc'anzi il GDPR disciplina in dettaglio solamente le sanzioni amministrative, pertanto di natura pecuniaria, senza fissarne un valore minimo: all'art. 83 si dispongono molteplici criteri atti ad orientare il Garante nella quantificazione della sanzione stessa, fra cui:

a. La natura, la gravità ed altresì la durata della violazione, tenendo in considerazione la natura, l'oggetto o la finalità del trattamento nonché il numero di interessati lesi e il livello del danno da essi subito;

b. Il carattere doloro o colposo della violazione;

c. Le misure adottate dal titolare o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d. Il grado di responsabilità del titolare o del responsabile del trattamento, tenendo conto delle misure tecniche e organizzative da essi messe in atto;

e. Eventuali precedenti violazioni pertinenti commesse dal titolare o dal responsabile del trattamento;

f. Il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione;

g. Le categorie di dati personali interessati dalla violazione;

h. Eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso (si pensi a benefici finanziari conseguiti o perdite evitate).

Ai paragrafi 4 e 5 del medesimo articolo, il GDPR specifica poi che, accertata la violazione, la sanzioni amministrative pecuniarie possano arrivare fino a:

a. a) 10 milioni di euro, o per le imprese, fino al 2% del fatturato mondiale annuo dell'anno precedente, nei casi in cui, ad esempio, i dati personali vengano trattati in maniera illecita,

non venga nominato il DPO *(Data protection officer)* o non venga comunicato un data breach all'Autorità Garante;

b. b) 20 milioni di euro, o per le imprese, fino al 4% del fatturato mondiale annuo dell'anno precedente, nei casi più gravi quali l'inosservanza dei diritti degli interessati o il trasferimento illecito di dati personali ad altri Paesi.

Riassumendo, le possibili conseguenze per le organizzazioni che agiscono in violazione del GDPR comprendono sia sanzioni amministrative, che sanzioni penali, come anche condanne al risarcimento del danno ed eventuali misure correttive (si pensi al sopracitato divieto temporaneo di trattamento dei dati personali).[144]

Allora, considerate tali ripercussioni, si intuirà l'importanza di interpretare correttamente le disposizioni Regolamento ed, in particolare, il suo "DNA di fondo", ossia il sopracitato principio di *accountability* (traducibile come principio di responsabilizzazione).[145]

Sulla base di tale obbligo di rendicontazione spetterà infatti al titolare del trattamento adottare (e rispettare) tutte le misure tecniche, organizzative e legali necessarie a garantire l'effettiva protezione dei dati personali, consapevole che su di lui stesso, ed in minor parte anche sul responsabile del trattamento, graverà l'onere di documentare e dimostrare ex post la conformità di ogni misura adottata alla normativa Ue.

La chiave per interpretare correttamente la disciplina europea risiede proprio nel termine "dimostrare": un buon titolare del trattamento farà in modo che ogni misura, ogni procedura, ogni metodologia applicativa sia affidabile, credibile e giustificabile *ex post*.

---

144 L. Smoraldi, M. Strazzullo, "Prevenire è meglio che curare: il compito dell'avvocato in caso di data breach", in *Data Protection Law: diritto delle nuove tecnologie, privacy e protezione dati personali* - Rivista online Giuridica Semestrale, n. 2, 2021, p. 73.

145 Intervento di Luca Bolognini, Presidente dell'Istituto italiano per la privacy, avvocato ICT Legal Consulting, al Convegno Privacy Unolegal , Milano, 14 Giugno 2017.

Per far ciò risulta necessario sviluppare una forte sensibilità informatica, tecnologica e legale, imparando a valutare in modo appropriato le proprie decisioni, servendosi ad esempio di una *Gap Analysis*, ossia l'effettuazione di una mappatura completa dei trattamenti, confrontando le misure adottate con i principi stabiliti dal GDPR e verificando l'eventuale sussistenza di difformità , in modo tale da, eventualmente, intraprendere azioni correttive di adeguamento.

4.3.1 Simulazione: una breccia in sanità

Si sono definiti i data breach come eventi di violazione della sicurezza di una banca dati, che possono trovare derivazione tanto da semplici errori umani (commessi, ad esempio, nella fase di progettazione od implementazione di un software) quanto, ed è ciò che in questa sede più interessa, da sofisticati attacchi informatici ad opera di cyber criminali.

Si può parlare in tali casi di una "falla" (o per l'appunto, breccia): ossia una fessura nella quale l'hacker può insinuarsi ed avere accesso non autorizzato ai dati personali di un individuo, quali possono essere i dati sulla salute.

L'ambito sanitario infatti, formato da strutture che archiviano ed elaborano un quantitativo considerevole di informazioni sensibili sui pazienti, si presenta, ancor più di altri settori, obiettivo vulnerabile agli attacchi informatici.

Si voglia di seguito, per amor di chiarezza, presentare una simulazione, in ambito ospedaliero, di quelli che possono essere i possibili scenari scaturenti da un data breach, quali: il furto dei dati sanitari, l'eliminazione dei dati stessi e la loro alterazione. [146]

Tizio in tarda serata viene ricoverato per una colecisti, all'arrivo in ospedale viene immediatamente sottoposto a trattamenti ed esami sanitari il cui esito viene

146 E. Limone, "Sanità digitale: scenari scatenati da un data breach", in *Agendadigitale.eu*, Editore ICT&Strategy, Gruppo Digital360, Milano, 1 Luglio 2019.

registrato in una cartella clinica a disposizione del medico che lo visiterà il giorno seguente. Durante la nottata tuttavia, un gruppo di hacker riesce a "bucare" ed intromettersi nel sistema informatico ospedaliero, grazie ad alcune chiavette USB, contrassegnate appositamente dal logo ospedaliero, precedentemente lasciate in alcune postazioni del reparto col fine di esser scoperte ed in seguito installate dal personale. Gli infermieri infatti inserendo, erroneamente, le *pendrive* hanno dato immediato innesco al virus informatico artefice della "breccia" nel sistema ospedaliero. [147]

Durante la notte i cybercriminali si sono dunque connessi al *database*, dove risiedono registrati i dati sanitari di tutti i pazienti, inclusi quelli di Tizio.

Ed ecco così delinearsi i possibili scenari, lesivi rispettivamente dei tre principi cardine della triade CIA, ossia confidenzialità, disponibilità ed integrità :

Scenario 1. La sottrazione del dato. La mattina seguente i dati di Tizio vengono trovati correttamente dal medico curante che procede così con anamnesi, diagnosi e cure appropriate. La degenza ospedaliera di Tizio viene metodicamente seguita, fino alle sue dimissioni definitive.

Tutto procede regolarmente fino a quando però il reparto ICT, dotato di un sistema di tracciamento dei dati correttamente configurato, si accorge dell'avvenuto data breach e del conseguente furto di dati perpetrato.

Ecco che, in conformità alla normativa europea sopra ricordata, verrà redatta e notificata la segnalazione al Garante Privacy contenente gli elementi essenziali richiesti ex art. 33 GDPR (natura della violazione, numero degli interessati coinvolti, le misure adottate per porvi rimedio, etc.).

Da tale momento l'Autorità garante nazionale, in base al principio di *accountability*, darà avvio all'iter procedurale di controllo e valutazione in merito all'accaduto, vagliando le misure tecniche ed organizzative poste in essere dal titolare del

147 Indipendent Security Evaluators, *Securing Hospitals: a research study and blueprint,* 23 February 2016, p.39

trattamento, iter che potrebbe culminare in un provvedimento amministrativo sanzionatorio, laddove si accertasse una effettiva violazione o un non adeguamento alla disciplina Ue in materia di trattamento dei dati personali.

Si noti come in tale primo scenario non vi siano conseguenze strettamente cliniche pregiudizievoli per il paziente Tizio, questi ha subito infatti unicamente un danno derivante dalla perdita del controllo sui propri dati personali, una lesione della propria riservatezza.

A tal proposito l'art 82 GDPR prevede che *"chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento"*.

Ciò significa che il soggetto danneggiato (ossia l'interessato), a seguito di un trattamento dei propri dati in violazione della normativa GDPR, potrà ottenere il risarcimento di qualunque danno occorsogli, agendo per l'intero indifferentemente contro il titolare o il responsabile del trattamento, tenuti solidalmente al risarcimento (eventuali clausole contrattuali di ripartizione del danno varranno difatti solo nei rapporto interni tra i danneggianti stessi).

A proposito della risarcibilità del danno la Suprema Corte di Cassazione ha, in una recente pronuncia,[148] ribadito come il danno non patrimoniale, pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali, tutelato dall'art. 2 Cost. e dall'art. 8 CEDU, non si sottrae alla verifica della *"gravità della lesione"* e della *"serietà del danno"*. Da una lettura congiunta allora dell'art. 82 GDPR e della pronuncia della Suprema Corte emerge con chiarezza come, ai fini della risarcibilità del suddetto danno, siano necessarie in primis l'esistenza di una violazione del Regolamento 2016/679 e a seguire la dimostrazione dell'entità del danno stesso (nei due aspetti della gravità e della serietà).

In riferimento alla risarcibilità del danno viene poi precisato nel Considerando 146 del Reg. Ue che: *"Il titolare del trattamento o il responsabile del trattamento do-*

148 Cass. Civ, sez. I, sentenza 12 Novembre - 31 Dicembre 2020, n. 29982.

vrebbero risarcire i danni cagionati ad un soggetto da un trattamento non conforme al presente regolamento, ma dovrebbero essere comunque esonerati da tale responsabilità se dimostrano che l'evento dannoso non sia in alcun modo ad essi imputabile".

Si ricordi come l'art. 24 GDPR e il *Considerando* 74 stabiliscano che il titolare debba mettere in atto, previa valutazione della natura, ambito e finalità del trattamento nonché del grado di rischio, le misure tecniche ed organizzative adeguate, prescrivendogli inoltre di esser in grado di dimostrarne l'efficacia.

L'imputabilità del titolare allora dovrà necessariamente esser valutata alla luce dei principi di responsabilizzazione e *accountability* del GDPR, il titolare (o il responsabile) potrà fornire la prova che il danno si è verificato perché non poteva esser previsto, dato che esulava dalla propria possibilità di controllo (si pensi al caso fortuito o alla forza maggiore) o che sono comunque state opportunamente predisposte tutte le misure tecniche e organizzative per evitare che il danno potesse verificarsi.

Scenario 2. L'eliminazione dei dati. La mattina seguente i dati sanitari di Tizio non vengono trovati, ciò provoca un immediato allarme nel reparto e gli esami clinici vengono ripetuti con urgenza: Tizio subisce perciò un ritardo nel trattamento, ciononostante le sue condizioni mediche non sono gravi. I dati questa volta vengono ritirati "a mano" e si procede con le cure del caso. L'eliminazione dei dati allerta ad ogni modo il reparto ICT che procede ad una diagnostica da cui viene rilevata una eliminazione non autorizzata del dato sanitario: il database viene dunque scansionato ed il sistema bonificato.[149]

Si è assistito anche in tal caso ad una compromissione dei dati personali che ne ha causato una perdita della loro pronta disponibilità, per cui si vedrà ex art. 33 GDPR la stesura e la notifica al Garante privacy dell'avvenuta violazione degli stessi dati sanitari dei pazienti. Da qui prenderà avvio il regolare iter di accerta-

149 Per bonifica informatica si intende quel procedimento tramite cui si evidenziano intromissioni illecite all'interno di un sistema informatico.

mento e di valutazione da parte dell'Autorità di controllo nazionale in merito alla sicurezza del sistema informatico ospedaliero, vagliandone le misure tecnico-organizzative adottate.

In tale secondo scenario non vi sono parimenti danni seri al paziente, ma si registra comunque un discreto esborso di denaro al fine di pagare le risorse incaricate di sistemare la parte software, nonché ripristinare il corretto livello di sicurezza informatica.

Scenario 3. L'alterazione dei dati. La mattina seguente i dati di Tizio vengono letti dal medico curante che, preoccupato per i valori completamente fuori norma, suggerisce una terapia con un farmaco che peggiora le condizioni del paziente. Da questo momento la salute di Tizio si aggrava celermente, i medici comprendono che vi è una discrepanza fra i risultati riportati nel sistema e le risposte biologiche del paziente. Non trovando una corrispondenza Tizio viene sottoposto ad ulteriori esami clinici per poi, successivamente, vedersi corrisposte le corrette cure ed i trattamenti opportuni.

Rendendosi comunque conto del danno arrecatogli, dovuto ad una non corretta protezione della integrità dei propri dati sanitari da parte della struttura sanitaria, che con molta probabilità non aveva adottato tutte le adeguate misure tecnico-organizzative per prevenire il pericolo di data breach, Tizio si vede intenzionato ad agire per ottenere un risarcimento ex art. 82 GDPR.

Nel frattempo, si apre anche una fase di accertamento della sicurezza dei sistemi informativi dal lato del Garante che, accertato il data breach e il non adeguamento alla normativa europea sulla protezione dei dati, emette un immediato provvedimento con annessa sanzione amministrativo-pecuniaria. Il reparto ICT intanto effettua una riprogettazione dei sistemi di gestione del dato e della sicurezza, andando ad incidere ulteriormente sui costi da sopportare.

Ci si accorgerà di come il terzo scenario sia con probabilità quello con i costi di gestione maggiori, ma soprattutto, di come sia l'unico ad aver realmente messo a rischio la salute del paziente. L'alterazione del dato è sicuramente molto meno

visibile e rilevabile rispetto alla sua cancellazione o al suo furto e questo non fa che peggiorare i ritardi nelle reazioni del reparto ICT.

A tal proposito il tempo di rilevazione di un data breach risulta di dirimente importanza: al di là invero del caso in cui sia il malintenzionato stesso a render edotte le vittime circa l'effettuata violazione dei sistemi (spesso, come si vedrà, per chiedere un riscatto al fine di ripristinarne il regolare funzionamento), i tempi generali per suddetta rilevazione risultano ad oggi comunque molto alti.

Ovvio è pertanto che riuscire a monitorare i sistemi e le attività in modo tale da avere la piena capacità di accorgersi di una violazione in atto risulta il requisito imprescindibile per arrivare a prevedere, mitigare, nonché contenere tutti i possibili rischi informatici. [150]

A questo punto della trattazione appare comprensibile incominciare a domandarsi i motivi che si celano dietro a tali cyber-condotte, per quale ragione i dati sanitari siano tanto ambiti e soprattutto che concreto valore abbiano: se questi infatti sono un obiettivo criminale, significa che esiste una domanda di tali dati, e se c'è una domanda deve esserci un ritorno sull'investimento.

Si possono richiamare a tal proposito le parole di Agostino Ghiglia, componente del Garante per la protezione dei dati personali: *"Ad oggi il settore meno preparato risulta essere proprio quello sanitario che, tra l'altro, paga il prezzo di gran lunga più caro dal momento che la spesa per i data breach è notevolmente aumentata. È evidente che il comparto sanitario risulti essere il più bersagliato a causa della quantità e qualità dei dati custoditi e che, ovviamente, hanno un notevole valore economico. Gli attacchi criminali non mirano infatti solo a bloccare i sistemi dietro la richiesta di un riscatto, ma soprattutto a capitalizzare i dati sensibili. È fondamentale per questo motivo che le strutture sanitarie prevedano un piano operativo d'azione che racchiuda sia una difesa in ambito tecnologico*

150 C. Telmoni (intervento), al talk "Cybersecutity per la sanità digitale: conoscere per non rischiare", andato in onda il 28 Ottobre 2021, nella prima giornata di FORUM PA Sanità, evento digitale organizzato da FPA e P4I-Partners4Innovation.

che un piano formativo del personale dal momento che il più delle volte gli attacchi vengono veicolati con precise comunicazione e-mail". [151]

4.3.2 Il mercato nero della salute

Vanno moltiplicandosi gli studi e le indagini che si interrogano sul perché il rischio cyber imperversi così minacciosamente sul mondo della sanità e, in particolare, sul mercato dei dati sanitari nel *dark web,* [152] al fine di comprendere struttura, profitto ed acquirenti di un fenomeno mondiale così in profonda crescita.

Di seguito si riportano le parole di Soro: *"Si tratta del commercio di dati tra i più delicati, in quanto in grado di rivelare gli aspetti più privati della vita, ed espressivi, oltretutto di una condizione di particolare vulnerabilità quale è quella di un paziente ricoverato in ospedale. Che è dunque affidato ad una struttura pubblica, dalla quale deve potersi aspettare non soltanto attenzione e cura, ma anche un assoluto rispetto per la propria riservatezza e dignità".* [153]

Innanzitutto si premetta come il valore di tali dati sensibili sia strettamente legato alla loro stessa tipologia, essi invero possono includere: dati personali identificativi del paziente, indirizzi e-mail, numeri di tessere sanitarie, varie informazioni mediche (esami diagnostici, referti di laboratorio, prescrizioni di medicinali etc.), dati assicurativi, nonché attestati e certificati di laurea in medicina. Risulta in questa sede opportuno rifarsi al report *"Healthcare Cyber Heists"* condotto dalla società statunitense di cybersicurezza Carbon Black, datato al 2019. Il rapporto si fonda su un campione di interviste, rivolte a venti manager *CISOs,* [154] ossia sog-

---

151 Intervista a Agostino Ghiglia, componente del Garante per la protezione dei dati personali, "La sanità la più colpita. Proteggere reti e dati sensibili", di Luigi Garofalo, 9 Novembre 2021.

152 Il termine *dark web* indica un insieme di contenuti e servizi della Rete nascosti ai motori di ricerca, necessitanti di appositi programmi per essere raggiunti.

153 Intervista ad Antonello Soro, presidente dall'Autorità Garante per la privacy dei dati personali, "Il Garante: un caso di straordinaria gravità", riportata sul *Corriere della Sera* - Ed. Bergamo, 31 Ottobre 2013, di G. Ubbiali

154 Si noti come CISO sia l'acronimo di *Chief Information Security Officer.*

getti responsabili del definire e sviluppare strategie di sicurezza informatica, in tal caso specificatamente nel settore sanitario.[155] È fuor di dubbio che tale *survey* offra unicamente una prospettiva parziale, ma ad ogni modo rilevante per comprendere quanto siano frequenti le cyber-offensive, come vengano rubati i dati sanitari e successivamente venduti.

Si vogliano dapprima riassumere i risultati chiave scaturenti dal rapporto:

a. L'83% delle organizzazioni sanitarie intervistate ha notato un notevole aumento dei cyber attacchi nell'ultimo anno (riferendosi al 2018);

b. I tentativi di intromissione informatica sono stati, in media, 8.2 al mese per ogni *endpoint*, ossia non per ogni organizzazione, ma per ciascun dispositivo connesso alla Rete;

c. Il 66% delle organizzazioni ha affermato che le offensive non sono solo più numerose ma anche maggiormente sofisticate, testimoniando di esser state bersaglio sia di attacchi *ransomware* che *island hopping*;[156]

d. All'interrogativo su quale sia la maggiore preoccupazione della propria organizzazione le risposte sono state: la compliance (33%), i limiti di budget e risorse (22%), la perdita dei dati sanitari (16%) la vulnerabilità dei *medical devices* (16%) e l'impossibilità sopraggiunta di accedere ai dati dei pazienti (13%). Da qui si ricavi forse uno dei maggiori problemi della sicurezza sanitaria: pensare che la *compliance* (traducibile col termine "conformità") equivalga alla sicurezza. Troppe organizzazioni, seppur considerate conformi agli standard generali di sicurezza, sono ad ogni modo

---

155 R. McElroy, T. Kellermann, *Healthcare Cyber Heists in 2019: 20 leading CISOs from the healthcare industry offer their perspective on evolving cyberattacks, ransomware & the biggest concerns to their organizations,* Carbon Black, June 2019.

156 Per *island hopping* si intende una tecnica di attacco informativo utilizzata dagli hacker per infiltrarsi nella rete informatica di una azienda sfruttando le strutture satellite, ossia tante organizzazioni più piccole e con standard di sicurezza IT maggiormente vulnerabili rispetto all'obiettivo principale. Ecco che, bucando la rete informatica del fornitore, l'hacker riesce a risalire fino alla rete dell'azienda target principale.

state vittime di molteplici violazioni: la conformità a disposizioni normative, regolamenti e codici di condotta è indubbiamente un buon punto di partenza, ma ciò non basta, è infatti necessario creare un programma di sicurezza atto a contemplare anche tutte le esigenze specifiche di una organizzazione.

Il rapporto prosegue poi stilando un borsino indicativo di quelle che sono le tipologie di dati sanitari maggiormente vendute sul dark web, disposte di seguito in ordine di valore:

a. I dati in assoluto più costosi, nonché di allarmante diffusione, sono i Provider Data, si possono cioè trovare online i "pacchetti Fullz" (Fig. 4.2) contenenti tutti i documenti di cui si necessita per ricostruire il background di un medico professionista: dati personali identificativi, diplomi di laurea, licenze mediche, nonché documenti assicurativi. Il costo del "pacchetto" si aggira sui 500 dollari. Si intuisce già la versatilità che tali dati garantiscono nel loro utilizzo: dal procurarsi farmaci soggetti a prescrizione medica (per un uso personale od altresì per rivenderli in rete), fino all'acquisire falsi documenti (passaporti, patenti di guida etc.) con cui un qualsiasi soggetto non qualificato possa porsi come medico nei confronti di organizzazioni come assicurazioni e servizi sanitari. Ciò che accade dunque vede in primo luogo un hacker compromettere la rete di un fornitore di servizi sanitari al fine di ricavarne documenti amministrativi che possano supportare l'identità contraffatta di un medico, cosicché successivamente un qualsiasi acquirente possa, a proprio vantaggio, presentarsi con la falsa identità del medico *de quo*.

A seguire le parole del Professor Kevin Curran, dell'università di Ulster: *"Dire che i dati dei pazienti siano dalle 10 alle 15 volte più preziosi dei dati inerenti alle carte di credito è una buona stima, dato che tali dati offrono ai criminali informazioni*

permanenti ed altamente fruttifere".[157] Ovvio è che nel caso di una carta di credito rubata, questa possa essere istantaneamente disattivata e gli addebiti fraudolenti contestati. Negli ultimi anni poi le banche hanno notevolmente rafforzato la propria sicurezza online incorporando trasferimenti e transazioni più sicure. Nel mondo sanitario il tutto risulta più complesso: i dati rubati non sono facilmente recuperabili e, in verità, non si dispone nemmeno di un chiaro processo per aiutare i pazienti a fronteggiare le conseguenze del furto di identità. È pertanto indispensabile prevedere delle misure proattive al fine di ridurre le probabilità che tale dati vengano trafugati.

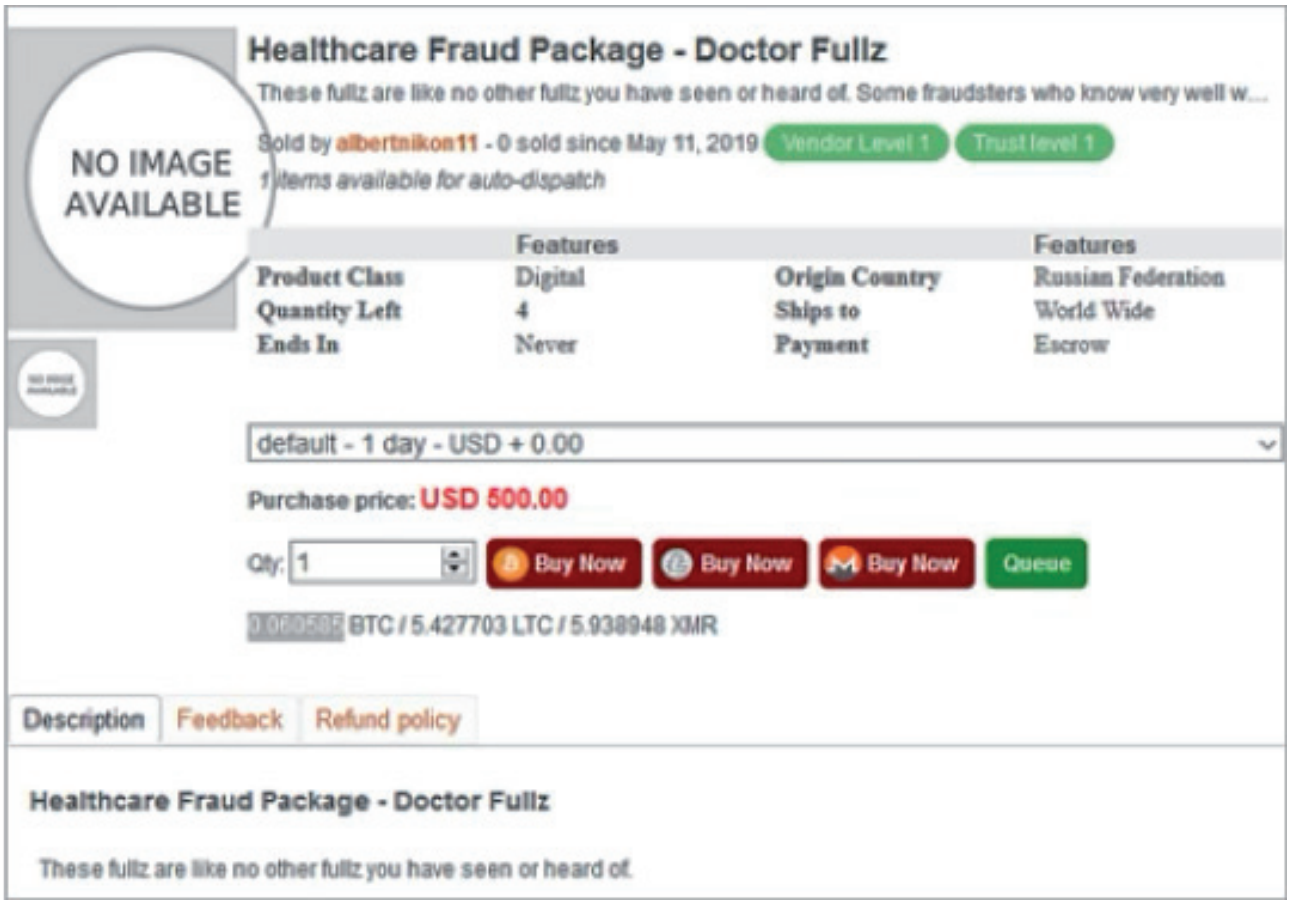

Fig 4.2 Annuncio di vendita su AlphaBay, avente ad oggetto un completo pacchetto Fullz "Healthcare Fraud Package", al prezzo di 500$. Fonte: report Carbon Black, "Healthcare Cyber Heists in 2019".

157 N. Griffin, Health correspondent, "Patient data 10-15 times more valuable than credit card data", in *Irish Examiner*, May 19 2021.

b. Altri contenuti sanitari rinvenuti nella *darknet*, più numerosi e meno costosi dei precedenti, sono i *forgeries* (o falsificazioni), venduti ad una fascia di prezzo compresa fra i 10 e i 120 dollari. Essi possono assumere la forma di tessere sanitarie contraffatte, come anche di false prescrizioni mediche (Fig. 4.3). Ad un venditore possono difatti esser forniti tutti i dati necessari per realizzare una *prescription label* personalizzata per l'acquirente, con cui ad esempio possa superare i controlli (quali in aeroporto) che vietano il trasporto di alcuni farmaci senza specifica prescrizione medica.

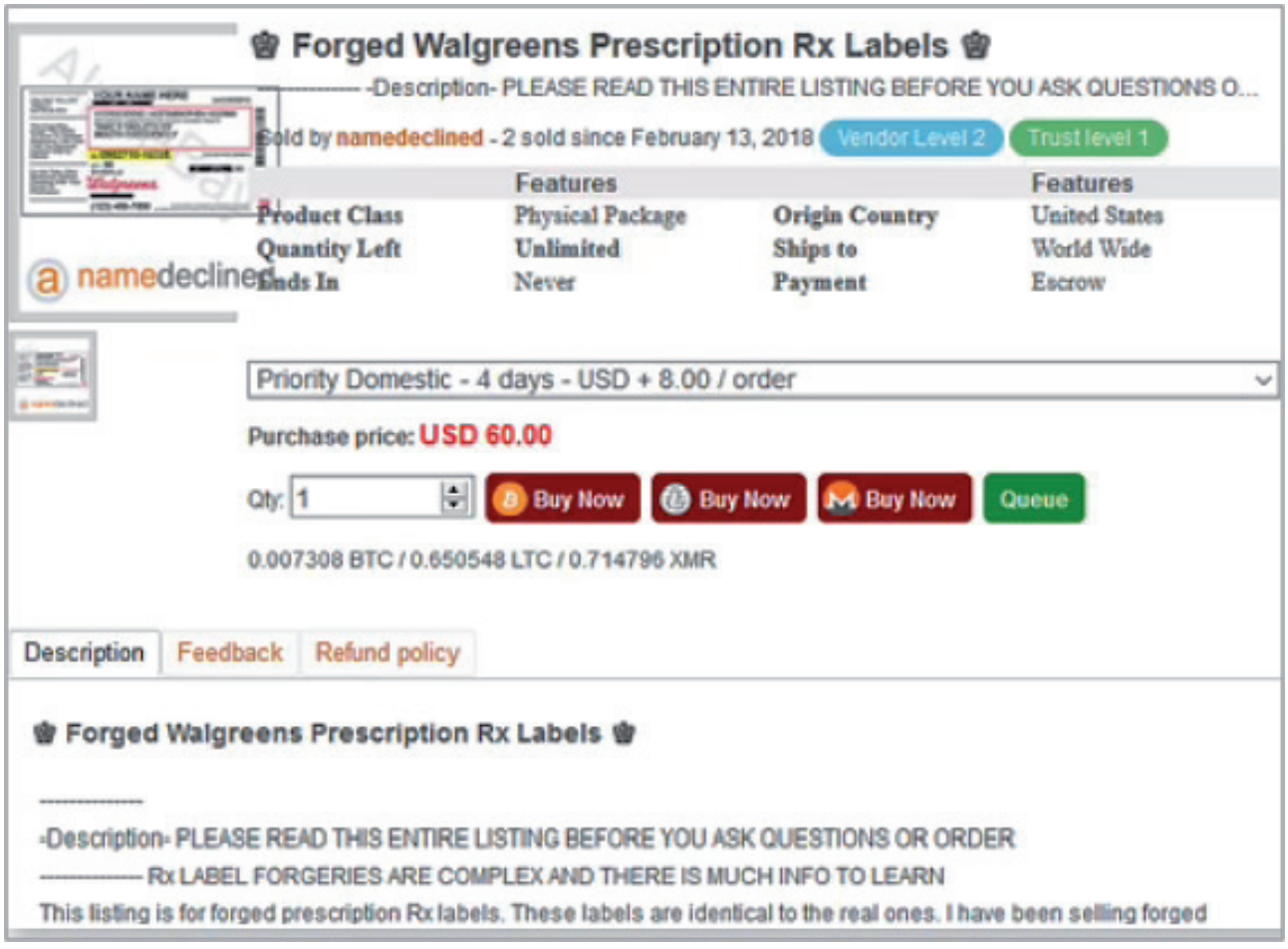

Fig 4.3 Annuncio di vendita su AlphaBay, avente ad oggetto prescrizioni contraffatte di farmaci Walgreens, al prezzo di 60$. Fonte: report Carbon Black, "Healthcare Cyber Heists in 2019".

c. Ancora si possono trovare *insurance login information,* ad un prezzo contenuto di 3.25 dollari per singola credenziale di accesso, il basso costo è dovuto alla rapidità con cui le medesime credenziali possono esser cambiate una volta che la compromissione del database viene scoperta. Comunque, una volta ottenute le informazioni di accesso, l'acquirente può ottenere illecitamente tutte le informazioni riguardanti una determinata assicurazione medica, utilizzabili a loro volta per ricevere cure mediche o medicinali sotto prescrizione. [158]

Si vogliano qui riassumere i fini a cui si può indirizzare il furto dei dati sanitari: la costruzione di false identità, la commissione di frodi ai danni dei sistemi assicurativi, la richiesta di somme di denaro come riscatto al fine di rientrare in possesso dei propri dati, la contraffazione di documenti (certificati di nascita, passaporti etc.), l'emissione di false ricette mediche, nonché l'ottenimento di determinati farmaci.

Non si può nemmeno escludere che fra gli acquirenti nel suddetto sistema di compravendita vi siano anche grandi aziende, interessate parimenti ad entrare in possesso di Big Data altrimenti irraggiungibili, si pensi a grandi imprese farmaceutiche che potrebbero sfruttare i pacchetti di dati medicali in vendita per la ricerca e lo sviluppo di nuovi farmaci, avvantaggiandosi così notevolmente sulla propria concorrenza.

Si sottolinei invero come dai dati sanitari, in una loro forma aggrega, sia possibile derivare, predittivamente, una conoscenza circa: le aspettative di vita di una popolazione, la futura necessità di cure, assistenza o medicinali, la suscettibilità di sviluppare determinate patologie, tutte informazioni altamente sfruttabili per orientare determinate politiche e scelte commerciali ad opera di grandi *competitors*. [159]

---

158 Per ulteriori immagini esemplificative si rimanda al report di Trend Micro, *Cybercrime and Other Threats Faced by the Healthcare Industry,* Mayra Rosario Fuentes Forward-Looking Threat Research (FTR) Team, 2017, pp.13-17

159 Intervento Prof. Matteo Bonfanti, al convegno "Cybersecurity e protezione dei dati personali nella sanità: un nodo strategico per l'interesse nazionale", Fondazione ICSA in partnership con Link Campus University, 16 Giugno 2022.

Chiaro è comunque come i dati sanitari protetti di ciascun individuo, quelli che identificano ogni nostra storia di salute individuale, stiano diventando ad oggi miniera d'oro per i cyber criminali.

Così Roberto Setola dell'Università Campus Bio-Medico di Roma: *"I dati sanitari sono i più appetibili per i cyber criminali. Sul dark web infatti sono quelli che vengono venduti al prezzo più elevato, ciò è dovuto alla loro grande versatilità: possono infatti risultare redditizi sia vendendoli sia utilizzandoli, sempre da un punto di vista criminale, contro il soggetto a cui appartengono. [...] Il problema maggiore è che i dati sanitari non sono ben protetti: il passaggio dalla carta al digitale negli ospedali e nelle strutture sanitarie non è stato accompagnato da un cambiamento culturale degli operatori della sanità esponendo così i dati ad un alto rischio di perdita, furto, nonché alterazione."* [160]

4.3.3 Caso: Ulss 6 Euganea di Padova

Si voglia qui brevemente ricostruire un recente caso di cronaca, al fine di comprendere quanto siano attuali gli argomenti di cui si va trattando e di che ampio raggio siano, penisola italica inclusa. Il tutto ha inizio il giorno 3 Dicembre 2021, momento in cui cominciano a diffondersi in rete le prime notizie riguardanti un attacco informatico subito dalla Ulss 6 Euganea, ossia l'Unità locale socio sanitaria di Padova. [161]

Non tarda ad arrivare un comunicato da parte della medesima struttura: *"L'Ulss 6 Euganea informa che nella notte si è verificato un attacco hacker, che ha comportato il blocco della maggior parte dei server, compromettendone la fruibilità. Stiamo intervenendo con la massima celerità con tutti i nostri tecnici informatici al fine di ripristinare il prima possibile i servizi."*

---

160 V. Franzellitti, G. Cavalcanti, intervista a Roberto Setola dell'Università Campus Bio-Medico di Roma durante la seconda giornata del convegno "Big Data in Health", riportata in *Sanità Informazione,* 3 Ottobre 2019.

161 Notizia riportata sui giornali locali quali *Padovaoggi*, "Attacco hacker Ulss 6 Euganea, pubblicati oltre 9.300 documenti", 16 Gennaio 2022.

I criminali hanno agito tramite attacco ransomware, di cui si avrà modo di trattare in seguito, rendendo impossibile accedere alle banche dati ed inviare informazioni alle piattaforme sanitarie, sospendendo le nuove registrazioni dei pazienti, il sistema dei laboratori, alcuni punti tamponi e hub vaccinali.

Di qui le immediate ripercussioni: i padiglioni di tamponi e vaccini (si pensi che in quel periodo si registravano più di 800 positivi in 24 ore a Padova e provincia) hanno dovuto riprendere a lavorare in modalità cartacea, e diversi problemi sono stati riscontrati al pronto soccorso, nelle terapie intensive, nelle radiologie, nei cup e nei laboratori analisi.

Così informa l'Ulss *"È in essere una collaborazione stretta con l'Azienda ospedaliera Università di Padova e con il privato accreditato, ai quali vengono convogliati i casi indifferibili. Ove non supportati da reti informatiche esterne, l'Azienda procederà provvisoriamente alla registrazione su supporto cartaceo, che potrà creare inevitabili rallentamenti."*

Inutile dire come si sono adoperati e hanno lavorato strenuamente oltre 60 tecnici del settore al fine di contrastare il blocco, di minimizzare i danni, nonché di bonificare tutte le macchine ospedaliere e certificare quelle "pulite".

Ad una settimana dall'attacco tuttavia soltanto un terzo dei computer risulta bonificato, ed i problemi persistono: seri danni vengono riscontrati alle infrastrutture IT, non risulta possibile emettere ricette dematerializzate, non possono essere inseriti i dati relativi agli isolamenti domiciliari da Covid-19, sono stati chiusi i punti prelievo e bloccate le prenotazioni specialistiche.

Solo in data 20 Dicembre si percepisce una lenta ripresa, si hanno difatti i primi risultati positivi (quali la riapertura di alcuni punti prelievi), al contempo però cominciano a diffondersi notizie circa una colossale mole di dati sensibili e di credenziali di accesso trafugati, il cui valore di mercato risulta incalcolabile: ecco profilarsi la probabile vera finalità dell'attacco informatico.

Con l'inizio del nuovo anno, dopo circa un mese da quello che è stato uno dei più gravi attacchi alla sanità italiana, sopraggiunge così la rivendicazione dell'attacco da parte del gruppo hacker *Lockbit 2.0* che, in un post, avvia una sorta di

"countdown": i dati sottratti dall'azienda sanitaria saranno resi pubblici il giorno 15 Gennaio 2022, salvo pagamento di un riscatto (la somma pareva ammontare sugli 800.000 euro in criptovalute).

Viene dunque immediatamente aperta da parte del Garante della privacy una istruttoria per il data *breach*, processo mirante a verificare se i dati in possesso dell'Ulss fossero adeguatamente protetti e se sia stato fatto tutto il possibile (ossia adottata ogni misura tecnico-organizzativa necessaria) per evitare che i dati venissero sequestrati ed eventualmente diffusi dai criminali informatici.

Come preannunciato, nel pomeriggio del 15 Gennaio, *Lockbit* pubblica i dati sanitari, e più precisamente vengono diffuse due cartelle dal nome "Ulss2" e "Ulss3" contenenti all'incirca 9.300 documenti (fra cui pdf, documenti excel, word, etc.) riportanti svariate informazioni: dati sensibili dei pazienti (referti medici, analisi, esiti di tamponi molecolari Covid, coi rispettivi dati anagrafici) tabelle illustrative di stipendi e turni ospedalieri del personale medico-sanitario, nonché informazioni sul budget dei vari reparti e tanto altro ancora.

Non è da escludere che ciò che sia stato divulgato sia solo una quota delle informazioni in possesso del gruppo hacker *Lockbit*, il quale potrebbe aver nel frattempo rivenduto un'altra importante porzione di dati *nell'underground* del web.

Da parte dell'Ulss è stato emesso di conseguenza un conclusivo comunicato ufficiale [162] in cui si legge: *"Fino ad oggi non sussisteva alcuna certezza che i malviventi fossero riusciti a venire in possesso di informazioni, in che quantità e il loro genere. I criminali avevano avanzato una richiesta di riscatto in denaro in cambio della non pubblicazione delle informazioni a loro dire sottratte all'Azienda Ulss 6. Tentativo estorsivo prontamente denunciato alle forze dell'ordine e alla Procura della Repubblica. [...] La task force dell'Azienda Ulss 6, nel pieno rispetto delle indagini in corso, è al lavoro per valutare entità e tipologia dei dati pubblicati. Si ricorda che le informazioni comparse sul dark web sono altresì frutto di attività illegale e dunque chiunque intendesse consultarle o utilizzarle commet-*

162 Comunicato stampa relativo all'azienda Ulss n. 6 Euganea, 15 Gennaio 2022, Padova, consultabile integralmente al sito internet https://www.aulss6.veneto.it/mys/apridoc/iddoc/4703.

terebbe un reato [...] Il confronto e lo scambio di informazioni con la Procura della Repubblica e il Garante per la protezione dei dati personali è costante, siamo a disposizione dei nostri utenti e confidiamo che le indagini di Procura e forze dell'ordine, che ringraziamo per il supporto, permettano di individuare e fermare questi criminali".

Tirando le fila di tale vicenda si può meditare sui danni che ne sono conseguiti: oltre alle perdite economiche riflesse sia a livello regionale che di sistema sanitario nazionale ed al grave danno reputazionale e d'immagine in capo all'Ulss, non si può trascurare l'offesa subita dai pazienti e dai cittadini che si sono visti negare diversi servizi sanitari (si pensi ad una visita specialistica per una malattia degenerativa) o hanno comunque subito dei rallentamenti nelle ricevere le proprie cure.

I dubbi, c'è da dire, permangono: è stato avviato un programma cyber ad hoc e sono state intraprese azioni di miglioramento per scongiurare, l'altrimenti inevitabile, ripetersi di un simile attacco?

Utili risultano, a tal proposito, le parole di Pierguido Iezzi, CEO e fondatore della cyber security company Swascan:[163] *"Di base, per rendere sicura una struttura è necessario ridurne il livello di esposizione al rischio cyber. [...] Quanto affermato passa per l'adozione tout court dei tre pilastri della cyber security moderna: sicurezza predittiva, preventiva, proattiva. Bisogna implementare nel perimetro delle strutture un sistema di tecnologie e processi non solo in grado giocare "di risposta" agli attacchi, ma anche in grado di prevederli e anticiparli tramite l'utilizzo di sistemi quali la Threat Intelligence,*[164] *che sia associata all'expertise di un Centro operativo di sicurezza".*

---

163 Intervista a Pierguido Iezzi, pubblicata il 14.05.2022, ad opera di Massimo Canorro, sul quotidiano sanitario nazionale Nurse24.

164 Per *Cyber Threat Intelligence* (CTI) si intende una attività di raccolta di informazioni provenienti da varie fonti, in merito ad attacchi informatici che colpiscono o sono potenzialmente in grado di offendere la sicurezza di una organizzazione. Tale patrimonio conoscitivo acquisito viene poi utilizzato per attuare consapevolmente strategie ed azioni utili alla prevenzione, alla mitigazione e all'eradicazione della minacce, a partire da una corretta valutazione dei rischi.

4.4 Inquadramento giuridico: il reato informatico

Si è già potuto rimarcare, nello scorso capitolo, come la rivoluzione informatica abbia consentito la smaterializzazione della realtà fenomenica, con l'introduzione di oggetti privi di sostanza materiale (si pensi al semplice "dato" informatico), intangibili, componenti di una nuova e parallela realtà, quella virtuale. [165]

Tuttavia il progressivo ampliamento degli strumenti informatici e la loro capillare diffusione hanno presto, si è visto, provocato uno sviluppo patologico e distorto dei sistemi di informatizzazione, portando ad una evoluzione delle pratiche criminose: sono emerse molteplici forme delinquenziali nuove, tanto per le modalità di esecuzione, quanto per i beni materiali e giuridici coinvolti, divenendo sempre più urgente l'esigenza di sollecitare un intervento legislativo in materia di diritto penale dell'informatica.

Si avviarono di conseguenza primordiali riflessioni, ad opera di cultori del diritto, incentrate sulla possibile individuazione di nuovi beni giuridici prodotti direttamente dall'informatica, andando presto a delinearsi due orientamenti contrapposti. [166]

Secondo il primo indirizzo, assai diffuso in Europa, i nuovi delitti cibernetici non producevano inediti interessi meritevoli di tutela, bensì introducevano soltanto nuove modalità di aggressione di beni giuridici comunque preesistenti (per chiarire, secondo tale visione, la frode informatica altro non sarebbe che una truffa realizzata servendosi di un computer, e l'interesse aggredito rimarrebbe pur sempre, come per la truffa comune, il patrimonio). Tale corrente di pensiero mirava dunque a sostenere il cosiddetto "metodo evolutivo", e cioè la necessità di introdurre singole disposizioni specifiche, riferite all'informatica, all'interno delle normative penali previgenti, impendendo così il ricorso a procedimenti interpretativi di tipo analogico, non consentiti in sede penale.

---

165 T. Pietrella, "Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle Botnets", in *Discrimen* - Rivista di diritto penale, ISSN 2704-6338, 2.12.2021, pp. 2-7.

166 P. Galdieri, "Il reato informatico", in G. Marotta (a cura di), *Tecnologie dell'informazione e comportamenti devianti,* Edizioni Universitarie di Lettere Economia Diritto, Milano, 2004 , pp. 29-74.

Diversamente, per il secondo indirizzo dottrinario, sviluppatosi per lo più nei Paesi anglosassoni, le nuove tecnologie determinavano il sorgere di nuovi interessi suscettibili di tutela ed era pertanto auspicato un intervento normativo *ad hoc* specifico e autonomo (seguendo il metodo delle cosiddetta "legge organica"), in grado di disciplinare separatamente dalle normative previgenti l'intero fenomeno criminale. [167]

Per comprendere quale indirizzo sia stato in concreto adottato nel nostro ordinamento, occorre dapprima volgere lo sguardo alla evoluzione normativa in materia di criminalità informatica, costituita da molteplici interventi legislativi fortemente condizionati da indicazioni di fonte sovranazionale. [168]

Il legislatore italiano si è infatti mosso sulla spinta della Raccomandazione del Consiglio d'Europa del 1989 *"Sur la criminalité en relation avec l'ordinateur"* mirante a che i diversi Paesi instaurassero una stretta collaborazione per la repressione della criminalità informatica, in quanto sempre più contraddistinta da carattere sovranazionale.

Essa proponeva inoltre alle Nazioni aderenti due liste di *cybercrimes*: una cosiddetta "lista minima" comprendente fattispecie la cui incriminazione, in virtù della loro diffusione e gravità era ritenuta obbligatoriamente necessaria (fra cui la frode informatica, l'accesso non autorizzato ad una rete o sistema, il danneggiamento di dati o programmi) ed una "lista facoltativa", riguardante invece condotte punibili sulla base della discrezionalità rimessa a ciascun Paese, anche solo con strumenti di tipo amministrativo.

Il legislatore italiano ebbe così il giusto *input* per rivedere le proprie disposizioni penali in merito ai crimini informatici, dando forma, nello stesso anno, alla Commissione Callà, composta sia da giuristi che da esperti di informatica col fine di arrivare alla stesura di un compiuto disegno di legge, che fu approvato il 23 Dicembre 1993.

---

167 V. Frosini, *Contributi ad un diritto dell'informazione*, Liguori, Napoli, 1991, pp. 165 ss.

168 Comitato dei Ministri del Consiglio d'Europa, Raccomandazione *Sur la criminalité en relation avec l'ordinateur*, 13 Settembre 1989.

Tramite la sopradetta legge n. 547 del 1993 ("Modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica") si è potuto da un lato introdurre all'interno del codice penale nuove fattispecie delittuose (quali gli artt. 615-ter, quater e quinquies) e dall'altro modificare le fattispecie esistenti con il riferimento ai beni informatici (ad esempio, prevedendo che il delitto di attentato ad impianti di pubblica utilità, ex art. 420 c.p., riguardi anche l'ipotesi di danneggiamento o distruzione dei sistemi informatici o telematici di pubblica utilità o di dati in essi contenuti). [169]

Ne consegue allora come il legislatore italiano abbia optato per il metodo sopraricordato come "evolutivo", ritenendo che le tecnologie informatiche vadano ad incidere sulle modalità di aggressione a beni giuridici o interessi che rimangono purtuttavia invariati, ossia già oggetto di tutela nelle diverse parti del codice. Rispetto dunque ad altri Paesi, quali gli Stati Uniti o la Francia, che differentemente hanno dedicato ai delitti informatici leggi *ad hoc* e titoli appositi all'interno dei rispettivi codici, in Italia le nuove norme sono state inserite in diverse parti del Codice penale, ciascuna vicino alla previgente norma ritenuta simile.

Da qui la distinzione dei fatti criminosi che possono essere commessi nel *cyberspace* in due diverse categorie: i reati informatici "in senso stretto", che includono fattispecie che presentano espressamente, nella propria formulazione letterale, elementi descrittivi di modalità, oggetti, attività frutto della tecnologia informatica, ossia relativi a procedimenti di elaborazione automatizzata di dati (si pensi all'accesso abusivo "ad un sistema informatico o telematico"), ed i reati informatici "in senso lato", dove vi rientrano invece fattispecie che, pur non tipizzando espressamente elementi di natura tecnico/informatica, comprendono anche i fatti criminosi commessi nel cyberspazio, costituendo essi semplici forme di aggressione a beni giuridici già tutelati da norme incriminatrici comuni (si pensi al reato di sostituzione di persona,

169 Legge 23 Dicembre 1993, n. 547, *Modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica,* reperibile integralmente al sito internet https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1993-12-23;547.

integrato ad ogni modo qualora siano utilizzate le generalità di una diversa persona per creare un falso account tale da indurre taluno in errore). [170]

Ancora ulteriori riforme della legislazione penale sono state in seguito apportate dalla legge n. 48 del 2008, recante la *"Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 Novembre 2001 e norme di adeguamento dell'ordinamento interno",* per mezzo della quale sono state introdotte alcune modifiche allo stesso codice penale (con l'inserimento degli artt. 635-bis, 635-ter, 635-quater, 635-quinquies), al codice di procedura penale, e anche al D.Lgs n. 231/2001 prevedendo la responsabilità degli enti per un'ampia serie di reati informatici. [171]

Come evidenziato comunque nella relazione parlamentare relativa a suddetto disegno di legge *"la portata dell'adeguamento normativo da realizzare nel settore del diritto penale sostanziale è risultata modesta, essendo in molti casi già in vigore una disciplina esaustiva, anzi addirittura più incisiva di quella richiesta dalle disposizioni della Convenzione di Budapest medesima".*

Si osservi in conclusione come, volendo contrastare fenomeni legati al funzionamento delle tecnologie, il legislatore debba necessariamente fare i conti con modalità, oggetti e comportamenti di natura squisitamente informatica, ossia elementi indubbiamente ardui da trasporre sul piano normativo.

Il rischio comunque è che l'individuazione di particolari modalità d'azione, volte a dar veste giuridica a determinati fatti criminosi informatici, possa risultare una tecnica di normazione inefficace: il costante aggiornamento delle tecnologie impiegate potrebbe cioè far cadere in rapida desuetudine le norme incriminatrici di settore, insuscettibili di essere aggiornate di pari passo con il celere sviluppo tecnologico.

---

170 R. Flor, D. Falcinelli, S. Marcolini, *La giustizia penale nella "rete": le nuove sfide della società dell'informazione nell'epoca di Internet,* Edizioni DiPlaP, Milano, 2015, p. 101.

171 Legge 18 Marzo 2008, n.48, *"Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 Novembre 2001, e norme di adeguamento dell'ordinamento interno"*, per una lettura integrale si rimanda al sito internet https://www.gazzettaufficiale.it/eli/id/2008/04/04/008G0070/sg.

Per tali ragioni, si è scelto di adottare una tecnica di tipizzazione che, pur impiegando nuove terminologie, non si concentra tanto sulla tecnologia utilizzata, quanto si focalizza più in generale sulle finalità perseguite, o ancora, sugli eventi realizzati. È così che lo strumentario di diritto sostanziale adottato nel nostro sistema penale sembra esser in grado di apprestare strumenti di qualificazione giuridica sempre attuali.[172]

4.4.1 L'accesso abusivo ad un sistema informatico o telematico

Si passi ora ad una breve rassegna delle disposizioni normative che più possono inquadrare giuridicamente le condotte di Data breach per come ivi descritte.

L'esigenza di perseguire l'accesso abusivo a sistemi informatici emerse già alla fine degli anni '80 quando, precisamente nel 1989, suddetto reato fu inserito nella sopraricordata "lista minima" delle condotte informatiche abusive, proposta dal Consiglio d'Europa nella Raccomandazione sulla Criminalità Informatica, per poi esser così recepito nel Codice penale italiano con la legge n. 547 del 1993, seguendo l'approccio *"old wine in new bottles"*,[173] che contempla l'accostamento dei cybercrimes ai reati tradizionali.

Più nel dettaglio, con la legge 547/93 sono state introdotte all'interno della Sezione IV, capo III, del titolo XII del Codice penale, dedicata alla disciplina dei delitti contro l'inviolabilità del domicilio, tre disposizioni (gli artt. 615-ter, 615-quater, 615-quinquies) riguardanti, rispettivamente: l'accesso abusivo ad un sistema informatico o telematico, la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, nonché la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

---

172 E. Albamonte, "Il reato informatico nella prassi giudiziaria: le linee guida internazionali per il contrasto ai nuovi fenomeni criminali", in *Rivista Elettronica di Diritto, Economia, Management*, n.3, 2013, p.146-157.

173 S. Brenner, "Defining cybercrime: a review of state and federal Law", in R.D. Clifford, Cybercrime: *The investigation, prosecution of a computer-related crime*, Carolina Academic Press, Durham, 2006, pp. 15-104.

Ebbene si parta dall'art 615-ter ragionando in primo luogo sulla sua collocazione normativa, ossia nella parte del codice penale per l'appunto riservata ai delitti contro la persona, ed in particolare, nella sezione dedicata alla tutela del domicilio, come a voler dire che il sistema informatico vada in qualche modo assimilato ad una privata dimora.[174]

Nella relazione accompagnante il disegno della citata legge del 1993, il legislatore riconosceva espressamente come i sistemi informatici e telematici rappresentassero ormai *"una espansione ideale dell'area di rispetto pertinente al soggetto interessato"* a cui, dunque, estendere la tutela della riservatezza della sfera individuale, così come garantito dall'art. 14 della Costituzione.[175]

In tal modo si sono mossi i primi passi verso la formulazione della nozione di *"domicilio informatico",*[176] inteso proprio quale spazio ideale di pertinenza della persona (fisica o giuridica): i sistemi informatici e telematici, al pari del domicilio, rappresentano ambienti che devono rimanere riservati e conservati al riparo da ingerenze e intrusioni altrui, luoghi dunque inviolabili, delimitati da confini virtuali paragonabili a qualunque altro spazio privato, in cui un soggetto esplica liberamente la sua personalità in tutte le sue manifestazioni, ed esercita il proprio diritto allo *ius excludendi alios*.[177]

Di conseguenza l'art 615-ter (con una formulazione simmetrica rispetto all'art 614 c.p.[178]) punisce, nell'ipotesi base, con la pena della reclusione sino a tre anni, colui che si introduce abusivamente, o si mantiene contro la volontà espressa o tacita di chi ha diritto di escluderlo, in un sistema informatico o telematico protetto da misure di sicurezza.

---

174 Il domicilio, nel diritto privato italiano, corrisponde ex art. 43 c.c al luogo in cui una persona *"ha stabilito la sede principale dei suoi affari ed interessi"* , per tali intendendosi tanto quelli di natura personale, quanto quelli di natura sociale, politica ed economica

175 Art. 14 Cost. *"Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale".*

176 L. Levita, "La disciplina sostanziale: i reati informatici in senso stretto", in G. D'aiuto (a cura di) *I reati informatici: disciplina sostanziale e questioni processuali*, Giuffrè Editore, 2012, pp. 3-91.

177 Cfr. Cass. Pen. Sezioni Unite, Sentenza 26 Marzo 2015, n. 17325.

178 Art 614 c.p. *"Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di ci ha il diritto di escluderlo, ovvero si introduce clandestinamente o con l'inganno, è punito con la reclusione da uno a quattro anni".*

Stando a tale disposizione risulta passibile di esser punito tanto chi senza esservi autorizzato (da qui il carattere della abusività) [179] entra nel sistema altrui, che il soggetto, pur autorizzato, il quale si mantiene nel sistema oltre i limiti temporali e le modalità consentite: si noti come in entrambi i casi si venga puniti anche se l'introduzione nel sistema non comporti danni o manomissioni, in quanto bene giuridico protetto dalla norma non pare essere l'integrità del sistema informatico o la riservatezza dei dati ivi contenuti, bensì, come poi confermato dalle pronunce dei giudici di legittimità, [180] risulta tutelato il domicilio informatico, quale luogo riservato, nonché estensione naturale del domicilio materiale. [181]

Così come avviene infatti per la violazione di domicilio, che si consuma quando un soggetto si introduce nell'abitazione altrui senza il permesso, la violazione di domicilio informatico, si realizza nel momento in cui un soggetto abusivamente acceda al sistema altrui, risultando ad ogni modo irrilevanti, ai fini della sussistenza del reato, punito a titolo di dolo generico, le finalità specifiche (quali trarre profitto dall'ottenimento di informazioni riservate, o cagionare danni) che abbiano soggettivamente motivato l'ingresso nel sistema, salvo una loro rilevanza per integrare diverse ed ulteriori fattispecie criminose. [182]

Chiaro è infatti, e lo si è potuto capire discorrendo dei casi di Data breach, come l'accesso abusivo sia solitamente prodromico alla realizzazione di reati più gravi, come il danneggiamento di sistemi informatici, nonché connesso

---

179 Secondo alcuni autori l'espressione in parola sarebbe del tutto superflua e non aggiungerebbe nulla sotto il profilo interpretativo, poiché utilizzata al solo fine di far virare l'attenzione sull'antigiuridicità della condotta (Cfr. C. Piergallini, "I delitti contro la riservatezza informatica" C. Piergallini, F. Viganò, M. Vizzardi, A. Verri (a cura di) in *Delitti Contro la persona,* CEDAM, Padova, 2015, pag. 770). La stessa Corte di Cassazione ha criticato la locuzione "abusivamente si introduce" per la sua *"forte ambiguità e la conseguente possibilità d'imprevedibili e pericolose dilatazioni della fattispecie penale se non intesa in senso di accesso non autorizzato"*, Cass. Sez. V 17 Gennaio 2008 n. 2534.

180 Cfr. Cass. Sez. V, 26 Ottobre 2012, n. 42021; Sez. V, 31 Marzo 2016 n. 13057

181 C. Domenicali, "Tutela della persona negli spazi virtuali", in *Federalismi.it Rivista di diritto pubblico italiano, comparato, europeo*, ISSN 1826-3534, n. 7, 28 Marzo 2018, pp. 10-14.

182 Sul dolo generico richiesto si rimanda alla pronuncia della Cassazione sent. 2012, . 4694 secondo cui integra il delitto ex art. 615-ter c.p.: *"La condotta di colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto, violando le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema".*

alle ancora più frequenti richieste di pagamento di riscatti per ripristinare il sistema stesso violato.

Andando ad operare poi una analisi letterale della norma si aggiunga che una "introduzione", penalmente rilevante, in un sistema si concretizzi mediante la lettura dei dati ivi contenuti, o eventualmente una loro copiatura: [183] tali condotte, assieme a quella del "trattenimento" nel sistema, devono avvenire invito domino, ossia contro la volontà del titolare del diritto all'esclusione.

Ancora, mentre l'art 614 c.p. consente di tutelare qualsiasi abitazione o privata dimora, l'art 615-ter tutela soltanto quei sistemi informatici o telematici che risultano "protetti da misure di sicurezza", scelta questa non ampiamente condivisa dai commentatori, in quanto percepita da certi autori al pari di un "proteggo solo le abitazioni munite di una serratura antiscasso", senza contare che rimangono diversi problemi interpretativi circa cosa si debba intendere per misura di sicurezza.

Parte della dottrina ritiene che non si tratti di mezzi di protezione del luogo ove trovasi il computer (si pensi a lucchetti, porte, guardiani), ossia le cosiddette misure di sicurezza fisico-materiali, bensì mezzi di protezione aventi ad oggetto direttamente ed esclusivamente il sistema informatico o telematico, ossia le cosiddette misure di sicurezza logico-tecniche (si pensi alle *password*, o alla cifratura dei dati). [184] Altri, prendendo spunto dal fatto che si parli di misure di sicurezza al plurale, ritengono che una semplice parola chiave o un codice d'accesso non sarebbero sufficienti: le predette misure dovrebbero anzi essere intese come qualcosa di più complesso di una semplice password. [185]

Sembra comunque da preferire la tesi, accolta dalla giurisprudenza consolidata, secondo cui risulta sufficiente una qualunque misura di protezione, che sia an-

---

183 Cfr. Cass. Pen. Sez. V, 8 Luglio 2008, n. 37322, secondo cui il termine *"accesso"* deve intendersi non come collegamento fisico, ma logico: un superamento cioè della barriera di protezione del sistema che rende possibile il dialogo col medesimo, di modo che l'agente venga a trovarsi nella condizione di conoscere dati, informazioni e programmi.

184 R. Borruso, "La tutela del documento e dei dati", in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), *Profili penali dell'informatica*, Giuffrè Editore, Milano, 1994, p.29 ss.

185 G. Ceccacci, *Computer Crimes: la nuova disciplina dei reati informatici,* FAG, Milano, 1994, pag.70.

che banale e facilmente aggirabile, appunto perché la ratio sottesa all'inserimento di tale requisito è quella di richiedere un impegno effettivo, da parte dell'interessato, tenuto così a predisporre misure di sicurezza, quali elementi in grado di rendere esplicita e inequivoca all'esterno la propria volontà di riservare l'accesso solo a determinate persone.

Per quanto riguarda le non specificate nozioni di "sistema telematico ed informatico", queste sono volutamente lasciate in forma aperta dal legislatore, affinché possano essere inquadrate di pari passo e correlatamente allo sviluppo tecnologico.[186]

Per ciò che propriamente attiene alle nozioni di *tempus e locus commissi delicti,* seguendo la dottrina maggioritaria, si tratterebbe di reato istantaneo, consumantesi nel momento stesso in cui l'agente non autorizzato accede al sistema (o di reato istantaneo ad effetto permanente nell'ipotesi in cui questi vi permanga), ed in quell'esatto luogo in cui è presente il cosiddetto "terminale periferico", da cui il soggetto agente, quindi da remoto, digita le credenziali di autenticazione, esegue il login ed accede al sistema, superando le misure di sicurezza predisposte, risultando perciò assolutamente irrilevante il luogo fisico in cui si trova effettivamente il server centrale.[187]

In conclusione, si evidenzi come i commi secondo e terzo della norma in discorso contemplino alcune ipotesi aggravate, con rispettive sanzioni più severe, per quel che ivi interessa si noti come si abbia un incremento di pena qualora: dal fatto derivi la distruzione o il danneggiamento del sistema, o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento di dati, informazioni o programmi ivi contenuti; ed anche qualora i sistemi informatici o telematici in oggetto siano di interesse pubblico, quale chiaramente è il settore della sanità.[188]

---

186 Secondo la Convenzione Europea di Budapest sulla Criminalità informatica, stipulata il 23 Novembre 2001 *"computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".*

187 Cfr. Cass. Sez. Un., sent. 26 Marzo 2015, n. 17325.

188 Secondo la Cass. Pen. Sez. V, 21 Gennaio 2011, n. 1934 per aversi *"sistema informatico di interesse pubblico"* non è sufficiente la qualità di concessionario di pubblico servizio rivestita dal titolare del sistema, dovendosi accertare se il sistema stesso si riferisca ad attività direttamente rivolte al soddisfacimento di bisogni generali della collettività.

4.4.2 La detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Si è appreso come la riuscita di una intrusione in un sistema informatico dipenda in primo luogo dall'impiego di *password* e procedure d'accesso, passibili di essere rubate o scoperte con facilità.

Per tale ragione il legislatore è intervenuto in ottica preventiva, delineando una anticipazione della soglia della punibilità, configurando la fattispecie *de quo* quale reato di pericolo, ed andando così a sanzionare le condotte di detenzione e diffusione abusiva (ossia "illegittima") di codici di accesso, quali condotte oggettivamente prodromiche ad una successiva indebita intrusione nei sistemi informatici medesimi.

L'art. 614-quater risulta di notevole ampiezza, dal momento che delinea alternativamente come illecite non solo le condotte del procurarsi, riprodurre (ossia duplicare o creare autonomamente), diffondere (divulgare in modo indifferenziato), comunicare (render noto ad un numero chiuso di soggetti), nonché consegnare codici d'accesso, ma altresì il fornire indicazioni tecniche riservate od istruzioni idonee a svelare il metodo attraverso cui si possano aggirare, neutralizzare o superare le barriere di accesso al sistema, così da coprire ogni sorta di comportamento che possa consentire a terzi di acquisire la possibilità di accedere abusivamente a sistemi informatici, anche solo implementandone il patrimonio di conoscenze. [189]

In tutti i casi delineati, ai fini della sussistenza del reato, risulta necessario che tali condotte siano rette dal dolo specifico, consistente nel fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno. Va richiamata a tal proposito la nozione ampia di "profitto", elaborata dalla giurisprudenza per i reati contro il patrimonio, secondo cui tale vantaggio può essere anche di natura non strettamente patrimoniale (ad esempio qualora il soggetto agisca spinto da mero movente di soddisfazione morale).

---

189 G. Amato, V. Sandro Destito, G. Dezzani, C. Santoriello, *I reati informatici,* CEDAM, La biblioteca del penalista, Milano, 2010, pp. 89-96

Per quanto concerne poi il rapporto fra le due fattispecie incriminatrici agli art. 615-ter e 615-quater si è espressa recentemente la Corte di Cassazione, pronunciatasi per l'appunto su di un caso in materia di accesso abusivo a sistema informatico ed illecita acquisizione ed utilizzo di codici d'accesso.

Come spiegato nella pronuncia *"I delitti di cui agli artt.. 615-ter e 615-quater sono posti a tutela del medesimo bene giuridico, ovvero il c.d. "domicilio informatico", che l'art 615-quater protegge in misura meno ampia (ovvero limitatamente alla riservatezza informatica del soggetto) e l'art 615-ter più incisivamente, operando un più ampio riferimento al domicilio informatico tout court, quale spazio ideale di esclusiva pertinenza di una persona fisica o giuridica"*.

La Suprema Corte ha enunciato così il principio di diritto secondo il quale, poiché il delitto di detenzione di codici d'accesso costituisce l'antecedente necessario del più grave reato di accesso abusivo a sistemi informatici, in caso di contestazione dei due delitti in riferimento al medesimo contesto spazio-temporale ed in danno dello stesso soggetto passivo, il primo reato dovrà considerarsi assorbito nella seconda e più grave fattispecie. [190]

Ancora, similmente a quanto previsto per l'accesso abusivo, anche l'art 615-quater, al suo secondo comma, prevede sanzioni più severe qualora il fatto sia posto a danno di un sistema informatico o telematico utilizzato dallo Stato, o da altro ente pubblico o da impresa esercente pubblici servizi o di pubblica necessità, oppure altresì quando venga commesso con abuso della qualità di operatore di sistema.

La *ratio* dietro all'ultima ipotesi aggravata sopra elencata si rinviene nel voler punire più severamente comportamenti illeciti di agevole commissione, dato che l'operatore di sistema, in ragione delle sue funzioni ed attività, si trova in una evidente posizione di vantaggio dal punto di vista attivo, avendo la possibilità di accedere al sistema, alle sue aree riservate e di controllarne le operazioni.

---

190 Cfr. Cass., Sez. II, Sent. 14/01/2019, n. 21987: *"L'art 615quater, in quanto destinato a reprimere condotte prodromiche alla possibile realizzazione del delitto di accesso abusivo ad un sistema informatico o telematico, protetto da misure di sicurezza, e, quindi, pericolose per il bene giuridico tutelato dall'art. 615ter c.p., si atteggia quale necessario antefatto di detto reato, la cui latitudine lesiva sotto un profilo naturalistico necessariamente le presuppone e ricomprende".*

Si specifichi infine come vada considerato “operatore di sistema” non soltanto il tecnico che si trovi ad operare come programmatore o analista *sull’hardware* o sul *software* di un sistema informatico, ma anche qualsiasi soggetto che per le funzioni svolte si trovi ad intervenire su di questo stesso in forza di un titolo che glielo consente o glielo impone (si pensi ad un contratto per l’assistenza e/o manutenzione di un sistema informatico), volendosi sanzionare anche il tradimento della fiducia riposta dal titolare del sistema in chi professionalmente dovrebbe prendersene diligentemente cura.

4.4.3 La diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

L’elemento soggettivo del dolo specifico e la ratio di anticipare la protezione dei sistemi informatici vanno a connotare anche la successiva norma, di cui all’art. 615-quinquies, disciplinante una delle condotte maggiormente pericolose per l’integrità dei sistemi informatici, quale è la divulgazione di programmi informatici aventi effetti distruttivi (ipotesi tipica sono i c.d. *virus* informatici, frequenti cause di alterazione e danneggiamento dei sistemi in cui riescono a diffondersi e riprodursi).

Si conceda una breve digressione, senza pretesa di completezza.

Il *virus* è un programma caratterizzato dalla possibilità di espandersi e riprodursi all’interno del *software* in cui è stato inserito, “infettando” altri programmi e compromettendone la funzionalità. È solitamente di dimensioni molto ridotte (da pochi *byte* ad alcuni *kilobyte*) ed è specializzato per eseguire soltanto poche e semplici operazioni impiegando il minor numero di risorse, in modo da rendersi il più possibile “invisibile”. Un *virus* di per sé non è un programma eseguibile in maniera autonoma, per attivarsi invero necessita di un *software* ospite: il *virus* cioè inserisce una copia di se stesso nel file eseguibile, alterandolo, ed in questo modo quando un utente andrà a “lanciare” il programma infettato, dapprima verrà impercettibilmente eseguito il *virus* e poi, regolarmente, il programma stesso, e

mentre dunque l'utente vedrà, ignaro, l'esecuzione del programma lanciato, non si accorgerà del fatto che il *virus* sia attualmente in esecuzione e stia compiendo tutte le varie operazioni contenute nel suo codice. Programmi *virus* circolano in rete, come anche nei messaggi di posta elettronica, ma possono ugualmente essere contenuti in supporti esterni quali *floppy disk, pen drive, cd-rom e dvd*.

Sicuramente diverse possono essere le motivazioni sottostanti alla creazione e diffusione di programmi *virus*, dal comportamento semplicemente vandalico, a comportamenti di natura estorsiva, alla volontà di compromettere la funzionalità di sistemi informatici per ragioni concorrenziali o per interessi economici (si pensi a *virus* diffusi da tecnici informatici coscienti del fatto che vi sia la possibilità di esser chiamati a ripristinare l'efficienza del sistema).

Tornando alla norma de quo, anch'essa delinea una tutela preventiva, strutturandosi quale reato di pericolo astratto, dal momento che si prefigge di sanzionare condotte propriamente prodromiche rispetto ad un eventuale vero e proprio danneggiamento o malfunzionamento del sistema, che, laddove si realizzi, verrebbe tutt'al più punito ai sensi degli articoli 635-bis e seguenti.

Non vi è dubbio quindi che il reato si consumi anche se il programma nocivo non sia ancora stato inserito in alcun sistema informatico o non abbia ancora prodotto i suoi effetti, ma possieda in concreto le tipiche potenzialità distruttive, come nel caso di *virus* a tempo od attivazione collegata a particolari condizioni. [191] Suddetto arretramento della soglia di punibilità è determinato dal paradigma preventivo ad oggi dominante: se il fine del diritto penale è invero impedire eventi dannosi o pericolosi, è necessario anticipare la soglia della risposta punitiva allo stadio della realizzazione di atti idonei a determinare tali esiti infausti od addirittura a quella del presunto pericolo derivante da uno specifico comportamento. [192]

Altrettando ovvio è come tale operazione vada a collidere con l'assunto per il quale la sanzione maggiormente afflittiva della libertà personale dovrebbe soprag-

---

191 L. Cuomo. R. Razzante, *La nuova disciplina dei reati informatici*, Giappichelli, 2009, p.129.

192 M. Donini, *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà,* in A. Bernardi, M. Donini, V. Militello, M. Pasa, S. Seminara (a cura di), Collana quaderni di diritto penale comparato, Internazionale ed Europeo, Milano, Giuffrè editore, 2004, p. 104 ss.

giungere soltanto ove si accerti un fatto materiale connotato da reale disvalore e a condizione che non sia rintracciabile, nell'ordinamento giuridico nel suo complesso, un altro strumento in grado di arrecare efficace e pronta risposta al di fuori del diritto penale, dovendosi perciò tendenzialmente evitare i reati di mera disobbedienza e trovare rimedi giuridici alternativi per argine certe pratiche e comportamenti.

La disposizione in questione comunque, per come modificata ed ampliata dalla legge 48/2008, sanziona colui che abusivamente procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o in ogni altro modo mette a disposizione di altri apparecchiature, programmi, o dispositivi informatici vietati, il tutto allo scopo di danneggiare illecitamente un sistema informatico o telematico (o i dati ivi contenuti), ovvero di favorire l'interruzione, totale o parziale, od altresì l'alterazione del funzionamento del sistema medesimo.[193]

Si noti come per integrare la fattispecie criminosa possa bastare anche una consapevolezza ben minore del fine di distruzione o danneggiamento: a tal proposito infatti la Giurisprudenza di merito ha ritenuto sufficiente che vi sia l'accertata volontà dell'agente di diffondere il programma unita alla semplice consapevolezza dei suoi concreti effetti.

Opinioni discordanti in dottrina si registrano invece nei riguardi del bene giuridico protetto: secondo un primo orientamento la norma sarebbe posta a presidio del medesimo bene giuridico di cui agli artt. 615-ter e 615-quater, dotando così il domicilio informatico di una tutela rafforzata contro quelle condotte che, per la frequenza e la gravità dei danni che sono in grado di cagionare, rappresentano la minaccia maggiore alla sua integrità.[194]

Viceversa altri indirizzi di pensiero individuano il bene giuridico tutelato nella nozione di patrimonio (nella sua accezione di corretto funzionamento di un sistema

---

193 Secondo App. Bologna Sez. II, 27 Marzo 2008, sussiste il concetto di "alterazione" di un programma informatico quando lo si manipoli in maniera tale che compia azioni non volute dall'utente, ovvero si modifichino i parametri di funzionamento, anche secondo opzioni e possibilità previste nel programma stesso, contro la volontà dell'utilizzatore.

194 P. Galdieri, *Teoria e pratica nell'interpretazione del reato informatico,* Giuffrè editore, Milano, 1997.

informatico e di integrità dei dati ivi contenuti), in tal caso sarebbe stata allora più opportuna una collocazione sistematica della fattispecie all'interno del titolo XIII del codice penale (quale atto a disciplinare per l'appunto i delitti contro il patrimonio). [195]

In merito infine al rapporto fra l'art 615-quinquies e i reati informatici previamente trattati, si evidenzi come, in una sentenza di merito, si sia riscontrato il concorso proprio con l'art 615-ter di accesso abusivo ai sistemi informatici: il virus diffuso nel caso di specie aveva difatti consentito l'accesso ad un sistema informatico violandone le "barriere" protettive. [196]

Per quanto riguarda invece il rapporto con gli artt. 635-quater e quinquies (che verranno trattati nel dettaglio in seguito, in tema di attacchi *ransomware*), relativi al danneggiamento di sistemi informatici e telematici, ovvio è che vi sia una chiara interconnessione con la fattispecie de quo: in quest'ultima, quale reato di pericolo, le condotte previste verranno punite di per sé, prescindendo dalla verificazione del danno che, semmai, laddove in concreto realizzatosi verrà punito propriamente ex artt. 635- bis e 635-quater.

Si concluda sottolineando come i reati informatici sopra analizzati rientrino a tutti gli effetti fra i reati presupposto previsti dall'art 24-bis del D.lgs. del 2001 n. 231, per come modificato dalla legge 48/2008, ai fini della responsabilità penale degli enti: è stato infatti superato il principio per cui *societas delinquere non potest* ed è stato delineato come anche gli enti possano esser chiamati a rispondere dei reati posti in essere dai loro amministratori, dirigenti e dipendenti se realizzati nell'interesse o a vantaggio dell'ente medesimo.

All'esordio del suddetto del decreto legislativo (art. 1, comma II) si precisa tuttavia come le disposizioni in esso previste si applichino *"agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica", precisando al terzo comma che saranno viceversa esclusi da tale disciplina "lo Stato,*

---

195 G. Pica, *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999; F. Mantovani, *Diritto penale. Parte Speciale: I,* CEDAM, Torino, 2014.

196 Trib. Bologna, Sez. I Monocratica, Sent. 21 Luglio 2005, n. 11577

gli enti pubblici territoriali, gli altri enti pubblici non economici, nonché gli enti che svolgono funzioni di rilievo costituzionale".

Di conseguenza, ed è il motivo per cui si è voluto inserire l'argomento in trattazione, la dottrina correttamente esclude dal novero dei possibili destinatari della disciplina anche altri soggetti giuridici di natura pubblica che, pur non esercitando pubblici poteri, non si ritiene opportuno possano esser destinatari delle sanzioni indicate nel decreto legislativo n. 231, fra cui si evidenziano: le Aziende ospedaliere e le Aziende sanitarie locali. [197]

Quindi sebbene il D.lgs. 231/2001 possa applicarsi a tutti i soggetti privati del comparto sanità, in quanto inevitabilmente rientranti nelle definizioni di *"enti forniti di personalità giuridica/società e associazioni anche prive di personalità giuridica"* (quali case di cura, cliniche private, società che gestiscono strutture ospedaliere etc.), le problematiche applicative affiorano nella disciplina relativa agli enti pubblici.

Così infatti la Corte di Cassazione, con la sentenza n. 28699/2010 ha chiarito che *"il tenore testuale della norma è inequivocabile nel senso che la natura pubblicistica di un ente è condizione necessaria, ma non sufficiente, all'esonero dalla disciplina in discorso, dovendo altresì concorrere la condizione che l'ente medesimo non svolga attività economica. [..] Ogni società, proprio in quanto tale, è costituita pur sempre per l'esercizio di un'attività economica al fine di dividerne gli utili".* Per cui, pensando alle Aziende sanitarie locali, queste ultime ai sensi dell'art 3 del D.lgs. 502/1992 risultano qualificabili come enti pubblici operanti secondo le norme del diritto privato ed agenti con il principio di pareggio di bilancio, non risultando pertanto caratterizzate da finalità lucrative dovranno ritenersi escluse dall'ambito applicativo della 231. Pur tuttavia, in ambito regionale la tendenza rimane quella di recepire la disciplina 231 in una ottica di prevenzione da reato, ed anche quale ulteriore garanzia della migliore organizzazione e trasparenza delle PA. [198]

---

197 C. Pecorella, "Principi generali e criteri di attribuzione della responsabilità", In A. Alessandri & al. (a cura di), *La responsabilità amministrativa degli enti*. D. lgs. 8 giugno 2001 n. 231, Milano, pp. 65-89.

198 Così ad esempio la Regione Lombardia ha inteso mutuare i principi 231 ai fini dell'introduzione del Codice Etico e dell'implementazione del Modello Organizzativo nelle Aziende Sanitarie Locale ed Ospedaliere, formulando linee guida per l'analisi del rischio.

4.5 Profili di interdisciplinarietà: il Codice Privacy

Chiaro è che, inevitabilmente, in caso di commissione di reati informatici, si vadano ad intersecare profili di interdisciplinarietà con il trattamento illecito dei dati personali, tanto che una qualsiasi organizzazione, sia essa titolare o responsabile del trattamento, davanti, ad esempio, ad un accesso abusivo al proprio sistema informatico, dovrà avviare indagini interne al fine di verificare se vi sia stata anche una effettiva compromissione dei dati personali ivi trattati ed eventualmente aprire la regolare procedura per la gestione dei casi di violazione dei dati ai sensi dei, già visti in precedenza, articoli 33 e 34 del Regolamento Ue 2016/679.

Tra le varie tipologie di attacchi informatici infatti ve ne sono diversi caratterizzati sovente da una condotta di osservazione, illecita, delle abitudini del soggetto targettizzato, volta ad acquisire il maggior numero di informazioni possibili, così difatti argomenta K. D. Mitnick, noto informatico e hacker statunitense trattando del valore nascosto delle informazioni: *"qualunque tipo di informazione ha un suo valore economico, che sia poco utile o irrilevante, perché qualsiasi dato che entra in interconnessione con altri dati può consentire di risalire ad infinite informazioni sempre più importanti o significative"*. [199]

È dunque naturale che, affrontando il tema dei reati informatici, vengano in rilievo anche nozioni quali la tutela e la disciplina in materia di riservatezza e protezione dei dati personali. Si ripeta in questa sede che il Considerando 149, in combinato disposto con l'art. 84 del GDPR, sanciscano come i singoli Stati debbano stabilire le disposizioni concernenti le sanzioni penali applicabili per le violazioni del Regolamento Ue e delle norme nazionali attuative. Nel nostro ordinamento si è scelto così di mantenere in vigore quanto stabilito dal Codice della Privacy, emanato nel 2003, ed in particolare dagli articoli 167 e successivi, così come riformati dal d.lgs. n.101/2018.

Detta soluzione ha tuttavia restituito all'interprete un sistema caotico, ossia caratterizzato da continui rimandi tra normative eterogenee e da conseguenti pro-

---

199 F. Peluso, *La responsabilità nei nuovi reati informatici. Mezzi di ricerca e acquisizione della prova,* Maggioli Editore, Gennaio 2020, p. 180

blemi interpretativi nascenti dalla sovrapposizione di diverse fonti. Ne è scaturito cioè un corpus *iuris* connotato da sistemi sanzionatori disomogenei, passibili anche di entrare in conflitto fra loro, provocando un inevitabile *vulnus* ai principi di logicità, ragionevolezza, nonché al canone di proporzione. [200]

Infatti, come si vedrà, la scelta di utilizzare norme penali in bianco per sanzionare comportamenti lesivi della privacy mal si concilia con i principi di tassatività e di determinatezza che dovrebbero invece caratterizzare i precetti penali. La tecnica del rinvio poi rischia non solo di estendere eccessivamente l'ambito di rilevanza penale a fatti che sarebbero privi di quel disvalore, ma soprattutto, porta con sé il rischio che il rimando a norme secondarie renda l'opera di interpretazione della condotta vietata di estrema difficoltà tanto per l'interprete, quanto soprattutto per il cittadino che, come noto, dovrebbe invece conoscere il precetto prima della possibile commissione del fatto di reato, con conseguenze negative in termini di certezza del diritto e della pena. [201]

Si faccia a questo punto riferimento ad una delle più importanti norme del diritto penale della privacy, ossia l'art. 167 del Codice in materia di protezione dei dati personali che al primo comma punisce colui che, titolare o responsabile del trattamento, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, *"operando in violazione di quanto disposto dagli articoli 123* [202]*, 126* [203] *e 130* [204] *o dal provvedimento di cui all'articolo 129* [205] *arreca nocumento* [206] *all'inte-*

---

200 M. Solinas, "Tutela penale della privacy dopo il Gdpr: la frettolosa giustapposizione delle fonti è scaturigine di un sistema farraginoso che crea confusione, in *Responsabilità Civile e Previdenza*, fasc. 2, Vol. 85, 1 Gennaio 2020, pp. 663-688.

201 P. Balboni, F. Tugnoli, "Reati informatici e tutela dei dati personali: profili di responsabilità degli enti", in *Giurisprudenza Penale*, 2021/1-bis , pp. 3-8.

202 L'art. 123 disciplina le modalità con le quali risulta lecito, secondo il codice privacy, il trattamento dei dati di traffico.

203 L'art 126 si occupa di disciplinare il trattamento dei dati di ubicazione.

204 L'art 130 disciplina le c.d. "comunicazioni indesiderate" (si pensi alle comunicazioni di marketing).

205 Ex art. 129 *"Il Garante individua con proprio provvedimento, […] le modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico".*

206 Secondo Cass. Sez. 3, n. 40103 del 05/02/2015, per nocumento si deve intendere *"una concreta lesione della sfera personale o patrimoniale, direttamente riconducibile ad una operazione di illecito trattamento dei dati protetti".*

ressato". Ancora, ai sensi del secondo comma, è punito colui che, al fine di trarre per sé o per altri profitto ovvero arrecare danno all'interessato, *"procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento,* [207] *in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies* [208] *o delle misure di garanzia di cui all'articolo 2-septies,* [209] *arreca nocumento all'interessato"*.

Come sopra anticipato, si tratta di una norma penale in bianco in quanto non contiene una descrizione esaustiva delle condotte vietate, ma anzi, per l'identificazione del precetto vietato, fa rinvio a molteplici altre norme del Codice privacy, stabilenti criteri di liceità di determinati trattamenti di dati personali, la cui violazione andrà ad integrare la fattispecie de quo.

Oltre a ciò, talvolta la condotta a cui la norma fa riferimento è addirittura contenuta in altre disposizioni di rango secondario e di futura emanazione, o in provvedimenti generali del Garante, con le evidenti conseguenze, di cui già si accennava, in termini di *vulnus* ai principi di tassatività e di determinatezza della fattispecie.

In conclusione si ricordi come uno dei principi cardine del diritto penale sia il ne bis in idem, ossia il divieto di esser sottoposti a processo, o di essere puniti due volte, per il medesimo fatto. Da qui discende il problema del coordinamento fra le conseguenze previste dal GDPR (ed il procedimento innanzi al Garante), con le conseguenze penali ed il relativo processo.

Tale coordinamento risulta in parte gestito proprio dai commi 4 e 5 della fattispecie in esame, i quali si preoccupano di delineare, in via generale, le modalità di collaborazione tra i due soggetti: Garante ed il Pubblico Ministero.

Si prevede infatti che sia il Pubblico Ministero, alla ricezione della notizia di reato di cui all'art. 167, ad informare senza ritardo il Garante, e che sia viceversa quest'ultimo, nell'ipotesi in cui nel corso delle proprie attività ispettive rinvenga elementi

---

207 Il riferimento è al trattamento di particolari categorie di dati personali (che rivelino ad esempio origine razziale o etnica, opinioni politiche, ma anche dati biometrici e genetici).

208 Si riferiscono al trattamento di categorie particolari di dati personali, necessario per motivi di interesse pubblico rilevante (si pensi ai dati relativi a condanne penali e reati).

209 Si intendono le misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute.

da cui si possa presumere sussistente il reato, a trasmettere la relativa documentazione raccolta al Pubblico Ministero. L'Autorità Garante comunque, in virtù dei poteri autorizzativi e di accertamento riconosciuti ex lege, potrà partecipare alle indagini della Pubblica Accusa e svolgerne delle proprie, al fine di raccogliere elementi di prova.

È come se l'Autorità assumesse il ruolo atipico di "coordinatore tecnico" delle indagini preliminari: al termine infatti della sua attività istruttoria dovrà redigere un parere motivato da indirizzare al Pubblico Ministero, la cui decisione in merito all'esercizio dell'azione penale sarà inevitabilmente influenzata.

Entrambe le Autorità dovrebbero infine modulare le rispettive sanzioni, conformemente a quanto previsto dal *Considerando* 149 del Regolamento Ue e nel rispetto dello stesso *ne bis in idem*, ed in particolare al sesto comma viene prevista una riduzione della sanzione penale nel caso in cui sia già stata riscossa a carico dell'imputato una sanzione amministrativa pecuniaria. [210]

210 L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del D.lgs. 101/2018*, Giuffrè Editore, Milano, 2019.

B. RANSOMWARE

4.6 Le fasi di un attacco

Si proceda ora con la trattazione della cyber-minaccia principe fra gli attacchi informatici, che sempre più incombe sulle aziende di tutto il globo, sanitarie incluse.

Secondo le stime del, più volte ricordato, Rapporto Clusit 2021 [211] sulla sicurezza ICT, la diffusione degli attacchi di tipo ransomware è in significativa crescita, sia in termini assoluti che in termini di dimensione dei bersagli, che di ammontare dei relativi danni. Confrontando infatti i dati del Rapporto si ricava come nell'anno 2018 tali minacce rappresentassero il 23% di tutti i *malware*, per poi salire al 46% nel 2019, fino ad arrivare al 67% nel 2020, in pratica due terzi degli attacchi totali, relativi per l'appunto alla classe malware.

Il termine ransomware deriva dalla crasi delle parole inglesi *"malware"* [212] (programma malevolo) e *"ransom"* (riscatto), ed indica proprio un *malicious* software che, a seconda della sua tipologia, infiltrandosi in un singolo computer (o in una rete) può cifrare, occultare o negare l'accesso a dati o informazioni, come anche limitare od impedire l'accesso ad un sistema informatico, rendendo inutilizzabili documenti, archivi ed ogni altro contenuto memorizzato sul disco fisso, col fine di costringere la persona offesa a versare un importo in denaro per il riscatto del proprio *device* e per il ripristino dei dati. [213]

---

211 Rapporto Clusit 2021, op cit. supra a nota 52, pp. 26-30.

212 A sua volta il termine *malware* deriva dalla contrazione delle parole inglesi *"malicious"* e *"software"* e sta ad indicare programmi realizzati al fine di danneggiare i sistemi su cui vengono eseguiti o con l'obiettivo di sottrarre informazioni sensibili.

213 Il primo caso di ransomware risale al 1989. Il biologo americano Joseph Popp utilizzò il trojan AIDS (noto anche come *Aids Info Disk*), diffondendolo attraverso migliaia di floppy disk consegnati ai partecipanti ad un congresso sull'Aids (da qui appunto il nome del ransomware). Per ottenere la chiave di decifratura e rientrare in possesso dei propri dati, gli utenti dovettero pagare un riscatto di 189 dollari da inviare ad un ufficio postale di Panama.

Si riassumano di seguito le tre fasi che contraddistinguono un attacco ransomware, secondo quella che è la ricostruzione operata da Chris Goettl, *Vice President of Product Management for Security Products* di Ivanti, azienda specializzata in soluzioni di cybersecurity.

a. La contaminazione: per cifrare i dati di una specifica organizzazione, un attaccante dovrà in primo luogo trovare il modo di eludere le difese e le misure di sicurezza poste in essere dal soggetto *target*. A tal proposito, modalità più diffusa risultano essere le e-mail di *phishing*, quali indirizzate a profittare della scarsa attenzione e della mancanza di conoscenza degli utenti, risultando a tutti gli effetti il principale vettore di recapito del ransomware.

In dettaglio, con la predetta tecnica, sfruttante il social *engineering*,[214] si fa riferimento alla ricezione di e-mail fraudolenti provenienti, in apparenza, da mittenti conosciuti ed affidabili (si pensi ad istituti bancari od assicurativi), attraverso cui gli utenti: o sono persuasi a cliccare su di un link, rimandante a sua volta ad un' imitazione del sito web legittimo, ed a fornire, su richiesta, le proprie informazioni riservate (quali delle credenziali di accesso), o altresì sono portati a scaricare malware quali allegati, od ancora ad intraprendere altre azioni che ugualmente esporrebbero la propria organizzazione alla criminalità informatica (a furti di identità, violazioni di dati, attacchi ransomware etc.).

Si permetta allora una breve, quanto doverosa, riflessione.

La cybersicurezza non è solo un problema di tecnologia, bensì di persone: alle volte la più grande minaccia alla sicurezza di una azienda potrebbe celarsi non dietro ad un sofisticato virus

---

214 Per *social engineering* (o ingegneria sociale) ci si riferisce ad una tecnica di attacco cyber basata sullo studio del comportamento e della psicologia umana, così da sfruttarne debolezze e vulnerabilità, al fine di spingere gli individui *target* a compiere azioni avventate e contrarie ai loro migliori interessi. È una tecnica largamente utilizzate dagli hacker in quanto, si capisce, è indubbiamente più facile e meno costoso ingannare le persone (c.d. "hacking umano") che violare un computer od una rete.

né un ad un firewall installato male, quanto invece riscoprirsi nel fattore umano, nella sua disattenzione ed ingenuità. [215]

È sufficiente cioè che un dipendente, detentore di informazioni critiche, con una scarsa alfabetizzazione informatica, cada nel tranello degli hacker per rendere nullo un sistema di sicurezza avanzato.

Ed è proprio per questo motivo che le aziende dovrebbero ad oggi più che mai investire nell'idea di infondere una "cyber-cultura" mediante: formazione ed aggiornamenti periodici del personale (incentrati sulla consapevolezza dei rischi, sul valore delle informazioni, sulle procedure di sicurezza); una classificazione sistematizzata delle informazioni (suddividendole in confidenziali, interne, pubbliche etc.); nonché tramite *penetration test* (attraverso cui simulare attacchi di ingegneria sociale e verificare se i dipendenti adottino e rispettino effettivamente le misure di sicurezza previste). [216]

Ovviamente vi sono anche altre strategie utilizzate dagli attaccanti, quali vettori d'infezione ransomware, ad esempio tramite supporti rimovibili (si pensi ad una chiavetta USB o ad un hard disk) tale tecnica viene anche chiamata *baiting* (ossia "esca"), dato che, proprio come accade per le e-mail di *phishing*, mira a far leva sulle vulnerabilità del fattore umano, lasciando incustodito, in un luogo strategico, un supporto di memorizzazione contenente il software malevolo che si attiverà non appena l'oggetto stesso verrà collegato ad un computer.

Ancora, i criminali per intromettersi in una rete possono anche sfruttare le vulnerabilità note e non ancora *patchate* dagli amministratori (si pensi al celebre attacco *WannaCry* che sfruttava la vulnerabilità del protocollo SBM v1 sui sistemi Win-

---

215 K. Mitnick, *L'arte dell'inganno*, Feltrinelli, Milano, 2013.

216 A. Antonilli, op. cit. *supra* a nota 3, pp. 94-96.

dows), oppure possono ugualmente accedere alle reti tramite sistemi di *credential stuffing*, ossia usando combinazioni di login e password sottratte dai database, diffuse e reperite online sul dark web.

b. L'estrazione: una volta eluse le difese esterne, il passo successivo per l'attaccante è quello di studiare segretamente ed indisturbato il network aziendale, mappando i server e tutta la rete di protezione, al fine di individuare la collocazione dei database che custodiscono le informazioni critiche e sensibili, ossia quei dati per cui l'azienda target sarebbe disposta a pagare pur di poterli decriptare il prima possibile.
In questo momento entrano in gioco i sistemi EDR *(Endpoint Detection and Response)*, famiglia di strumenti tecnici composta da software di monitoraggio in grado di rilevare comportamenti sospetti, identificare una minaccia (la sua *root cause,* la sua portata etc.) provvedendo così al suo contenimento ed eliminazione, nonché capaci di operare un ripristino della rete alla normalità. [217]
Da soli però gli EDR potrebbero non essere sufficienti, per questo motivo a tali contromisure andrebbe affiancato un approccio di tipo zero trust (letteralmente "nessuna fiducia"), basato sull'assunto che nessun utente deve intrinsecamente esser ritenuto attendibile, per cui dovrà essere costantemente autorizzato prima di poter accedere ad una rete, ciò permette di scovare azioni sospette anche laddove queste siano riconducibile ad una utenza considerata al di sopra di ogni sospetto (come quella di un *admin*), ma ugualmente violata dall'attaccante. [218]

---

217 Kaspersky, *EDR & MDR: tutto ciò che occorre sapere: definizioni, funzionalità e vantaggi,* Kaspersky Lab., 2021, p.3

218 Zscaler, *Le tre chiavi per la trasformazione attraverso l'approccio zero trust: piattaforma, persone e processo, Zscaler* Inc., 2021.

c. La cifratura: nell'ultima fase i cybercriminali usciranno allo scoperto, realizzando il loro obiettivo: bloccare l'accesso al sistema informatico, cifrare i dati dell'organizzazione e chiedere il pagamento di un riscatto per ottenerne il ripristino. In particolare l'attaccante (spesso non si tratta di singoli hacker, ma di vere e proprie organizzazioni criminali), dopo aver criptato i file rendendoli irrecuperabili, farà comparire sulla schermata del computer della vittima una richiesta di riscatto (di regola in monete virtuali), corredata da dettagliate istruzioni circa le modalità di pagamento (in genere attraverso la rete TOR, ossia nel dark web).

In effetti, un ulteriore fattore che ha contribuito ad incrementare gli attacchi ransomware è stata proprio la progressiva diffusione delle criptovalute, sempre più utilizzate dai cybercriminali data la loro tendenziale pseudonimia [219] (ed in alcuni casi anonimità), che accorda loro di esser tracciati con maggiore difficoltà. [220]

Sempre più poi gli attacchi ransomware sono accompagnati da una componente ulteriore di esfiltrazione delle informazioni, idonea a compromettere quindi non solo l'accessibilità del dato, ma anche la sua confidenzialità: oltre al rischio di totale intellegibilità dei dati, il mancato pagamento del riscatto potrà in tal caso comportare la diffusione pubblica dei dati sensibili dell'entità colpita (si pensi al caso sopra analizzato, subito dalla Ulss 6 Euganea di Padova).

Si parla in tal caso di *Double extortion attack:* [221] termine co-

---

219 La maggior parte delle criptovalute infatti non sono anonime, ma pseudonime, in quanto la criptovaluta stessa all'interno di un portafoglio virtuale non è legata alle persone, ma piuttosto a una o più chiavi specifiche (o "indirizzi").

220 F. Di Geronimo, C. Maggia, "La gestione dei ransomware, un approccio multidisciplinare", in *Privacy& Data Protection, Technology, Cybersecurity,* n. 1, Aprile 2022, Egea, pp. 74-99.

221 La paternità di tale metodo va riconosciuta al gruppo criminale *Maze* che, a fine 2019, minacciò di utilizzare le informazioni sensibili trafugate come base per compiere ulteriori azioni malevoli, minacciando altresì la pubblicazione di tutti i file rubati fra cui risultavano presenti contratti, cartelle personali dei dipendenti e documenti riguardanti clienti.

niato dal fatto che l'organizzazione target si vede soggetta a due forme simultanee di estorsione, l'una mediante il blocco dei file crittografati e l'altra mediante la minaccia della pubblicazione dei dati sensibili. Tale tattica comporterà allora la notifica alla vittima circa un periodo di tempo (da pochi giorni a diverse settimane) entro cui pagare il riscatto, se la vittima si rifiuterà di versare la somma, i dati rubati saranno resi pubblici dopo la scadenza del timer, viceversa se verrà pagato il riscatto, sarà consegnata la chiave di decifratura e i dati esfiltrati saranno distrutti. Per caricare la vittima di maggiore pressione e per dimostrare di esser davvero in possesso dei dati, è diventato comune per gli attaccanti pubblicare online, prima della scadenza del sopradetto *countdown*, già una piccola quantità di dati altamente sensibili, a dimostrazione così della veridicità e della serietà di quanto minacciato. [222]

Ancora, a peggiorare ulteriormente il quadro, alcuni aggressori hanno ideato una nuova tipologia di estorsione, detta *Triple Extortion*, in cui non solo i dati vengono crittografati ed esfiltrati, ma nel caso in cui non si risponda al pagamento del riscatto, gli aggressori potrebbero lanciare altresì un attacco DoS o DDos [223] contro alcuni servizi della vittima, aggiungendo così un ulteriore fattore di stress ad un team di sicurezza già alle prese con le prime due estorsioni (si capirà, aumentare le tattiche di pressione significa aumentare anche la probabilità di profitto).

---

222 Exprivia, "Maze e ransomware as a service: sanità sotto minaccia della doppia e tripla estorsione", in *Cybersecurity360*, 22 Giugno 2021, pp. 2-5.

223 Con *Distributed Denial of Service* (DDoS) si indica una forma di attacco Dos, che tenta di rendere non disponibile un sito web o una risorsa di rete, sovraccaricandoli con traffico dannoso, proveniente non da un unico dispositivo ma da più computer appartenenti ad una *botnet* più ampia, *"stressando"* così i sistemi *target* al fine di renderli inutilizzabili.

Non è un caso che, nonostante ogni *industry* risulti essere possibile target di attacchi ransomware, questi colpiscano oggi, più che in passato, settori particolarmente data-sensitive, come per l'appunto quello sanitario, o enti che erogano servizi essenziali per la collettività (si pensi al settore bancario o assicurativo). La necessità infatti degli enti operanti in tali settori di poter accedere alle proprie informazioni comporta una maggiore propensione al pagamento del riscatto, di modo tale da evitare le conseguenze economiche e sociali devastanti che deriverebbero dalla perdita dei dati o anche solo dalla temporanea impossibilità di accedervi.

Alla luce di tutte le previe considerazioni risulta evidente come quella del ransomware si posizioni fra le minacce più preoccupanti, sia per società ed enti, che per le singole persone coinvolte: le organizzazioni vittime di attacchi potrebbero sì considerare di pagare gli ingenti riscatti al fine di proteggere la propria *business continuity,* senza tuttavia aver mai certezza circa l'onestà dei cyber criminali, i quali potrebbero, nonostante l'avvenuto pagamento, negare la consegna della chiave di decifratura dei file, pubblicare i dati aziendali sul web oppure sì regolarmente fornire la chiave promessa, ma al contempo installare componenti malevoli, lasciando così il sistema compromesso per futuri attacchi.

A ciò si aggiunga anche il dubbio relativo all'uso che i criminali medesimi possano fare del denaro ricevuto in seguito al riscatto, il cui pagamento pone inevitabilmente un dilemma di ordine non solo etico e morale, ma anche legale e reputazionale.

Volendo concludere, una corretta gestione della minaccia ransomware richiederà necessariamente un approccio multidisciplinare, in grado di spaziare dalla creazione di una *governance structure* tale da scongiurare la perdita di informazioni o il blocco dei sistemi interni, fino ad arrivare all'adozione di strategie *post-incident* [224] essenziali per garantire il contenimento delle perdite economiche derivante dall'interruzione dei servizi, dai furti di dati, nonché dalle sanzioni e dagli obblighi risarcitori.

---

224 Per *Cyber Incident Response* si intende, in questa sede, un "set" di azioni in risposta ad un attacco ransomware: quali un intervento di *immediate rescue,* finalizzato ad eliminare o impedire il prodursi delle conseguenze negative legate all'evento.

4.7 Una rassegna di casi in sanità

Si è già capito come gli attacchi ransomware possano avere molteplici effetti avversi su di una azienda: dal danno reputazionale, ai danni monetari, alla perdita di clienti, alla riduzione della produttività. E si sarà altrettanto intuito che, laddove un simil attacco venga sferrato sul settore sanitario, si verificheranno di conseguenza: l'impossibilità di accedere tempestivamente alle cartelle cliniche e ai dati sanitari dei pazienti, come anche severi ritardi nel prestare cure e trattamenti da parte degli operatori sanitari (spesso obbligati a tornare ad una modalità di lavoro "cartacea"), o ancora più lunghe degenze dei pazienti o loro trasferimenti in altre strutture ospedaliere, con ovvi riflessi dunque non solo per ciò che propriamente concerne la nozione di *security*, ma andando fortemente ad influire anche sul concetto di *safety*.

Si provino allora qui a riassumere le motivazioni che rendono le strutture sanitarie appetibili bersagli degli attacchi di tipo ransomware: *in primis* gli ospedali archiviano ed elaborano un quantitativo considerevole di informazioni sensibili e confidenziali sui pazienti (facilmente vendibili od utilizzabili per ottenere un elevato riscatto), *in secundis* sono altresì strutture particolarmente vulnerabili agli attacchi informatici, essendo dotate di sistemi, dispositivi e macchinari spesso datati, non aggiornati e non concepiti a prova di cybersecurity, nonché, da ultimo, si noti come la tipica pressione causata dallo scorrere del *countdown* ransomware si amplifichi notevolmente in ambito ospedaliero, dove vi è la consapevolezza che vedere in ostaggio applicazioni critiche e dati sensibili possa arrivare a mettere a rischio la salute, la cura, nonché la vita dei propri pazienti.

Si voglia ora calare quanto anzidetto nella realtà, operando una celere rassegna di alcuni, degli ormai innumerevoli, attacchi ransomware che hanno visto come proprio *target* il settore sanitario, al fine di comprenderne adeguatamente struttura, modalità operative, effetti e portata.

4.7.1 WannaCry

Si esordisca con quello che è ad oggi considerato il *cyber attack* più esteso mai lanciato, responsabile di una epidemia informatica su larga scala: durante il mese di Maggio del 2017 un insidioso attacco informatico, condotto attraverso la produzione e la diffusione del malware Wannacry ha colpito un elevato numero di server e sistemi informatici di imprese private, nonché di apparati statali dislocati nei diversi Stati. [225]

WannaCry è un ransomware della tipologia *cryptoworm*, ossia un particolare tipo di malware che rende inaccessibili (criptando, per l'appunto) i dati contenuti all'interno di un dispositivo, per cui l'utente si vedrà impossibilitato nell'accedere alle relative informazioni, e al contempo non potrà servirsi dei programmi installati al suo interno.

Una volta colpiti importanti server internazionali, principalmente mediante il ricorso alla tecnica offensiva (di cui sopra) del phishing, WannaCry si è poi propagato servendosi del funzionamento di un programma informatico in esso contenuto: *Eternal Blue*, [226] ideato con la specifica finalità di sfruttare i difetti, le lacune ed i limiti del protocollo SBM di Microsoft, ossia un protocollo utilizzato per condividere *files* e comunicazioni di varia natura tra diversi nodi di una rete.

In altre parole, all'interno di WannaCry, oltre che alla componente ransomware vera e propria, risultava presente anche un malware in grado di agevolare la proliferazione dell'attacco, infettando molteplici macchine in un lasso di tempo estremamente ridotto, sfruttando a tale scopo una vulnerabilità di Windows, presente in particolare nelle versioni 7 e 8 (si pensi come in tanti ambiti aziendali e istituzionali molti computer del 2017 usassero ancora versioni precedenti a Windows 10).

---

225 D. Mandrioli, "Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli stati", in *La comunità scientifica*, Fasc. 3/2018, Editoriale scientifica Srl, pp. 473-492.

226 Tale programma è definito dagli esperti come un "*exploit*" del protocollo SBM (Server Message Block) di Windows, intendendosi con tale espressione un programma in grado di conoscere e sfruttare le lacune e i difetti di un dato protocollo.

Con tale offensiva informatica dunque, dopo aver preso in ostaggio i computer infettati, si richiese il pagamento di un riscatto in denaro (nel caso di specie in *bitcoin*) per ottenere la risolutiva chiave crittografica.

Si è voluto qui richiamare tale attacco poiché, oltre a danneggiare un elevato numero di imprese private, è stato un grado di bersagliare anche numerosi organi statali, detentori di importanti funzioni collettive, in particolar modo paralizzando per diversi giorni il funzionamento del National Health Service del Regno Unito, proprio in ragione del fatto che gli ospedali vedevano l'utilizzo di migliaia di dispositivi non adeguatamente aggiornati (invero, fermi alla versione di Windows XP)

Si riporti quanto dichiarato da Brad Smith, Presidente di Microsoft Corporation, in un discorso pubblico datato al 10 Novembre 2017: *"A Maggio, l'attacco ransomware WannaCry ha colpito più di 200.000 computer in più di 150 paesi, mostrando al mondo intero l'ampio danno che le armi cyber-invisibili possono infliggere. Questo non ha causato solamente danni ai dispositivi informatici, ma ha avuto anche pesanti ripercussioni sui servizi da essi forniti. Il National Audit Office del Regno Unito infatti ha recentemente concluso una analisi sull'impatto di WannaCry, appurando come quest'ultimo abbia costretto il proprio Servizio Sanitario Nazionale a deviare le ambulanze e ad annullare oltre 19.000 appuntamenti di persone sia bisognose di ricevere esami medico-diagnostici, quanto di sottoporsi a interventi chirurgici. [...] WannaCry ha rappresentato un importante campanello di allarme nel mondo, mettendo in luce debolezze rilevanti per la sicurezza nazionale."*[227]

Provando dunque a riepilogare il panorama delle conseguenze subite in ambito ospedaliero, si può constatare come: il personale medico sia stato impossibilitato ad accedere ai sistemi elettronici, e di conseguenza ai dati dei pazienti; le apparecchiature mediche siano state (al pari d'altronde, degli operatori sanitari) scollegate dalla rete, causando così vari ritardi e disservizi; e ancora i pazienti, impossibilitati di ricevere le cure e i trattamenti dovuti, siano stati dirottati presso altre strutture sanitarie.

---

227 V. De Luca, G. M. di Sant'Agata, F. Voce, *Il ruolo dell'Italia nella sicurezza cibernetica: minacce, sfide e opportunità*, FrancoAngeli, Milano, 2018, p.43.

Certo non si è registrato alcun decesso direttamente collegato all'attacco, ma indirettamente si potrebbe, ragionevolmente, ipotizzare comunque un aumento del tasso di mortalità, dovuto ai rallentamenti subiti dagli ospedali nello svolgimento delle proprie regolari attività, nel prestare cioè cure e diagnosi (si immaginino le conseguenze che deriverebbero anche solo da 2,7 minuti extra impiegati affinché i pazienti sospettati di infarto miocardico ricevano un elettrocardiogramma).

Così Corrado Giustozzi, esperto di cybersecurity pubblica: *"Gli esperti lo annunciano ormai da tempo: attenzione che le vulnerabilità, e in generale la scarsa sensibilità cyber propria degli ambienti ospedalieri può arrivare a causare morti, oltre che danni economici ed inerenti alla privacy"*.

Sulla scia di queste ultime riflessioni, si prosegua con l'analisi di un ulteriore, nonché recente caso.

4.7.2 Ospedale Universitario di Düsseldorf

Secondo quanto riportato dalla stampa tedesca,[228] il 10 Settembre 2020, l'Ospedale Universitario di Düsseldorf (UKD) è stato vittima di un attacco informatico di tipo ransomware, atto a prendere di mira la vulnerabilità nel software Citrix. *L'iter* dell'attacco ha seguito il suo regolare andamento: i computer dell'ospedale sono stati resi inaccessibili (l'attacco avrebbe colpito all'incirca 30 server della struttura), i dati sono stati crittografati ed è infine sopraggiunta la richiesta di pagamento a titolo di riscatto.

Una prima peculiarità del caso *de quo* consiste nel poterlo classificare come un attacco "accidentale": lo stesso rapporto del ministro della giustizia tedesco ha riferito infatti come fosse in verità indirizzato verso l'Università di Düsseldorf, di cui tuttavia è parte anche la struttura ospedaliera, all'insaputa degli stessi hacker. La suddetta volontà di non colpire l'obiettivo ospedaliero sarebbe desumibile proprio dalla immediata collaborazione posta in essere, mediante l'invio gratuito

228 Si rimanda al quotidiano tedesco *Tagesspiegel*, reperibile al sito internet https://www.tagesspiegel.de/

della chiave di decrittazione, da parte degli stessi cybercriminali, una volta venuti a conoscenza delle conseguenze reali del proprio attacco: ossia il blocco dell'infrastruttura digitale dell'intero ospedale, il disservizio della rete, il rinvio o annullamento degli appuntamenti ed interventi chirurgici, nonché il trasferimento dei pazienti verso altre strutture.

Nonostante i suddetti sforzi da parte degli stessi autori criminali per annullare l'attacco, i sistemi informatici risultavano a tal punto compromessi, ed alcuni danni ormai irreparabili, di seguito occorre esser più chiari.

La notte dell'11 Settembre, i paramedici di Düsseldorf sono stati infatti avvertiti del deterioramento delle condizioni di una donna di 78 anni affetta da aneurisma aortico. A causa tuttavia dell'attacco informatico risalente al giorno precedente, che ancora riverberava i suoi effetti sul servizio ospedaliero, l'ambulanza che trasportava la donna in gravi condizioni mediche, è stata reindirizzata verso *l'Helios University Hospital* di Wuppertal, a più di 30km di distanza, il che ha ritardato di all'incirca un'ora le cure ed il soccorso della paziente, portandola al decesso.

Si capisce allora come la tragica sequenza degli eventi abbia fatto pensare di esser di fronte al primo caso di morte collegata direttamente ad un attacco informatico di tipo ransomware.

Tuttavia dopo un'indagine durata circa due mesi, il team di Markus Hartmann, Procuratore generale e Capo dell'unità centrale per la criminalità informatica di Colonia, concluse che non vi erano motivi sufficienti a reggere il nesso di causalità richiesto: è possibile sì che l'attacco informatico abbia, seppur minimamente, contribuito alla morte della vittima, ma ciò non è sufficiente per perseguire l'accusa di omicidio colposo, dato che lo standard di prova adottato in Germania richiederebbe ai Pubblici ministeri di dimostrare il "decisive role" dell'attacco stesso, ovvero di dimostrare l'inferenza logica per cui se non fosse stato per l'hacking, la vittima non sarebbe morta quella mattina.

In seguito invero a consultazioni con medici professionisti e dopo esser stata accuratamente predisposta l'autopsia, si ritenne che la gravità della condizione medica della vittima al momento del soccorso fosse tale che quest'ultima sarebbe ad ogni modo deceduta, indipendentemente dall'ospedale prescelto per il suo ri-

covero. Ciononostante, com'è ovvio, i cybercriminali rimangono perseguibili delle più tradizionali accuse di estorsione ed hacking.

Si è voluto inserire tale caso in trattazione perché pare essere un potente monito e campanello d'allarme per il futuro: l'impossibilità di ricevere cure può condurre a serie complicazioni coloro che richiedono servizi di emergenza, e così per chi che gestisce una infrastruttura critica (quale è quella ospedaliera) qualsiasi errore, disattenzione o trascuratezza nella protezione informatica potrebbe portare altresì ad esiti fatali ed irrimediabili, si potrebbe addirittura arrivare ad affermare, con le dovute cautele, che un sanità, non cyber-sicura, uccida.

4.7.3 Fatebenefratelli Sacco di Milano

Lo rivela *"Defending the Expanding Attack Surface"*, report sulle minacce informatiche relative al primo semestre 2022, a cura di Trend Micro Research: l'Italia si conferma ai vertici europei e mondiali dei Paesi più attaccati dai cybercriminali.[229] Nel primo semestre 2022 invero si classifica quale primo Paese europeo per numero di attacchi ransomware, posizionandosi settimo al mondo, nonché primo Paese europeo per attacchi *macro-malware*, e terzo al mondo. Tali posizioni così elevate nella suddetta "cyber-graduatoria" pongono i cittadini davanti alla sconfortante realtà relativa alla scarsa consapevolezza verso i rischi informatici: aziende e istituzioni si ritrovano ad esser costituite proprio da milioni di singoli utenti che aprono messaggi, condividono contenuti e usano dispositivi, senza comprendere o conoscere pienamente i rischi che ne conseguono.

Si capirà allora la necessità di concludere la suddetta rassegna di attacchi ransomware nel settore sanitario, spostando l'attenzione verso uno dei casi più recenti in territorio italiano.

L'allarme è scattato la mattina di Domenica 1 Maggio 2022: i sistemi gestionali

---

229 Trend Micro, *Defending the Expanding Attack Surface: Midyear Cybersecurity Report,* Trend Micro Research, global leader in Cybersecurity, 2022.

informatici dell'Asst Fatebenefratelli-Sacco, che ad oggi gestisce gli ospedali Sacco, Fatebenefratelli e Oftalmico, nonché il presidio ospedaliero Melloni, l'ospedale dei bambini Buzzi e varie strutture sanitarie e sociosanitarie territoriali , sono stati presi di mira da un attacco informatico di tipo ransomware che, travolgendo 500 server dell'infrastruttura principale, è riuscito a mandare in tilt l'intero sistema informatico, e conseguentemente i relativi presidi. [230]

In una prima nota diramata dall'Asst si legge: *"Si comunica che a causa di problemi tecnici all'infrastruttura informatica aziendale, i giorni 2 e 3 Maggio 2022 il Pronto Soccorso e i Punti Prelievo dei presidi ospedalieri dell'Asst Fatebenefratelli-Sacco non saranno in grado di accettare gli accessi dei pazienti. Per analoghe motivazioni potranno esserci gravi disagi anche nell'erogazione delle prestazioni ambulatoriali negli ospedali e nelle prestazioni presso le sedi territoriali. Sono stati allertati i servizi di sicurezza informatici regionali, nonché la Polizia Postale, che hanno inviato sul posto i propri specialisti per supportare le attività dei tecnici. Al momento non ci sono tempi definibili per il ritorno alla normalità."*

È solo poi con la nota ufficiale della Regione Lombardia che arriva la conferma circa la tipologia dell'attacco: *"Il disservizio è stato causato da un attacco informatico di tipo ransomware, causa della inutilizzabilità parziale dell'infrastruttura tecnologica"*.

Fra le dirette conseguenze subite, a questo punto della trattazione intuibili, si evidenzino: l'inaccessibilità alle cartelle cliniche dei pazienti (con il personale sanitario costretto a tornare al metodo cartaceo per le attività di refertazione, dimissione e prenotazione), il reindirizzamento delle ambulanze in arrivo al pronto soccorso verso altre strutture, l'irreperibilità di tutte le informazioni precedentemente archiviate (si pensi alle cure in svolgimento o ai medicinali somministrati), la limitata operatività dei punti prelievo, nonché generali rallentamenti, disservizi e ritardi nella prestazione degli stessi servizi sanitari.

Un aspetto preoccupante dell'attacco de quo è che i dati per accedere alla rete

---

230 Si rimanda a quotidiani locali, fra cui "Attacco hacker all'Asst Fatebenefratelli-Sacco: limitati gli accessi al pronto soccorso e ai punti prelievi", in *Regioni e ASL*, quotidiano online di informazione sanitaria, 2 Maggio 2022.

dell'ospedale (le credenziali d'accesso, per l'appunto) siano state messe in vendita *nell'underground* criminale almeno da Gennaio. Ciò significa che qualcuno è riuscito ad avere accesso ai sistemi della struttura ospedaliera prima di tale periodo, per poi avere il tempo di rivendere in seguito tali informazioni d'accesso a terze parti, ossia a coloro che poi hanno posto concretamente in essere l'attacco informatico.

Non è tardata a sopraggiungere la rivendicazione dell'attacco da parte del gruppo criminale *Vice Society* che, una volta scaduto il termine per concordare la somma del riscatto e in seguito alla minaccia relativa alla possibile pubblicazione dei dati esfiltrati, ha concretamente provveduto a quanto minacciato: la pubblicazione online di una vasta raccolta di documenti sensibili.

Fra i numerosi dati presenti in tale fuoriuscita sono stati identificati: dati sanitari dei pazienti (anche minori), carte di identità, documenti fiscali, tessere sanitarie, procedure interne, schede di valutazione dei dipendenti, contratti con i fornitori, istruzioni operative per il Covid-19, manuali informatici e scambi di email con i comitati etici.

Così Pierluigi Paganini, fondatore e *Chief Technology Officer* dell'azienda *Cybaze Spa*, una delle principali realtà italiane in cybersecurity: *"L'attacco di cui discutiamo è inquietante per molteplici motivi, in primis perché ad esser presi di mira ancora una volta sono i servizi di una struttura sanitaria. Purtroppo gli eventi degli ultimi mesi hanno dimostrato quanto sia basso il livello di sicurezza di molti ospedali italiani, con drammatiche ripercussioni sui pazienti"*.

4.8 Inquadramento giuridico: il danneggiamento informatico

Come si ricorderà, è con l'iniziale intervento organico in materia informatica, realizzato con la legge n. 547/1993, che è stata per la prima volta prevista una specifica fattispecie incriminatrice, l'art 635-bis c.p., diretta a sanzionare le condotte di

danneggiamento informatico, che in precedenza venivano ricondotte nella formula della più generale fattispecie incriminatrice di danneggiamento, ex art 635 c.p. [231]

A seguire, la tutela contro le aggressioni informatiche è stata fortemente rafforzata a seguito della legge n. 48/2008, destinata proprio ad implementare lo strumentario sanzionatorio diretto a punire le condotte che si risolvono in un attentato alla integrità dei dati o dei sistemi informatici, in precisa attuazione circa le indicazioni della Convenzione di Budapest del 2001.

Così ad oggi le norme cardine in materia risultano essere due: l'art. 635-bis e 635-quater c.p., che disciplinano, rispettivamente e separatamente, il danneggiamento di informazioni, dati e programmi informatici, ed il danneggiamento di sistemi informatici o telematici. Sono previste poi tutele rafforzate rispetto ad aggressioni particolarmente insidiose per la qualità delle informazioni o dei sistemi colpiti: l'art. 635-ter c.p. infatti punisce il danneggiamento di informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; l'art. 635-quinquies invece sanziona il danneggiamento di sistemi informatici o telematici parimenti di pubblica utilità.

È agevole intuire come i casi di attacco ransomware, di cui si è trattato in precedenza, rientrino proprio nelle anzidette fattispecie di tutela rafforzata, data l'alta sensibilità dei sistemi e dei dati colpiti, in quanto appartenenti al settore sanitario.

Grazie dunque al *novum* normativo introdotto dalla legge n. 48/2008, l'art. 635-bis è stato riformulato, andando, ad oggi, a sanzionare la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati e programmi altrui. [232] Si noti come a proposito delle condotte "cardine" di distruzione e deterioramento, si ritenga sussistente la prima qualora il reato venga commesso

---

231 G. Amato, "I reati informatici e le modifiche apportate dalla legge n. 48/2008", in G. Amato, V. Desposito, G. Dezzani, C. Santoriello (a cura di), I reati informatici, CEDAM, Mlano, 2010, pp.27-122.

232 È opportuno segnalare che giurisprudenza relativamente recente ha interpretato in maniera estensiva il concetto di "cancellazione" dei dati, affermando che essa possa consistere anche in una loro rimozione in via semplicemente provvisoria, rimediabile con un successivo intervento recuperatorio postumo, per cui "cancellazione" non equivarrebbe necessariamente ad una "irrecuperabile elisione" (Cass. Pen. Sez. V, 18 Novembre 2011, n. 2728).

avvalendosi di un mezzo fisico, viceversa il deterioramento richiamerebbe condotte più propriamente informatiche (quale la diffusione di virus), che ad ogni modo siano indirizzate ad alterare l'accessibilità, la fruibilità e il valore del dato stesso.

L'ampiezza della formulazione normativa mira proprio a dare copertura a qualsivoglia tipologia condotta (tanto fisica quanto virtuale), che si risolva in un pregiudizio, anche solo qualitativo, delle informazioni, dei dati o dei programmi informatici, non dovendo peraltro l'agente perseguire alcun fine specifico, ma, come richiesto dal dolo generico, solo avere la consapevolezza di distruggere, deteriorare, cancellare od alterare i suddetti beni informatici protetti. [233]

L'articolo *de quo* risulta collocato nel sistema codicistico all'interno della cornice dei delitti contro il patrimonio, ed in particolare dei delitti commessi mediante violenza alle cose o persone (Libro II, Titolo XIII, Capo I), per cui il bene giuridico meritevole di tutela risulta essere proprio l'integrità di un particolare aspetto del patrimonio, definibile per l'appunto "informatico", che a causa delle sue particolari caratteristiche, della sensibilità, e della rilevanza assunta nella società moderna si presenta non perfettamente omogeneo e riconducibile alle *res* tutelate dalla fattispecie di semplice danneggiamento ex art. 635 c.p. [234]

Per quanto riguarda poi la procedibilità del reato, quest'ultimo viene ordinariamente previsto come procedibile a querela della persona offesa, salvo quanto previsto, al secondo comma, circa le circostanze aggravanti di violenza alla persona o di minaccia, ovvero di fatto commesso con abuso della qualità di operatore di sistema, in tali ipotesi difatti il reato diviene procedibile d'ufficio.

Ad ogni modo non si dimentichi di mantenere uno sguardo d'insieme, in particolare rispetto a quanto detto circa l'inquadramento giuridico delle condotte di

---

233 Le "informazioni" costituiscono un insieme, più o meno ampio, di dati organizzati secondo determinata una logica; per "dato" si intende invece qualunque rappresentazione non interpretata di un fatto, codificato in modo da poter essere utilizzato tramite elaboratore; infine per "programma" deve intendersi una serie di istruzioni espresse attraverso un linguaggio comprensibile alla macchina, progettate al fine di ottenere un serie di prestazioni dall'elaboratore elettronico, così L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici,* Giappichelli Editore, Torino, 1 Maggio 2009, p. 205.

234 L. Stilo. "Il danneggiamento informatico: genesi e aspetti problematici della fattispecie, in *Diritto & Diritti,* Rivista Giuridica online, Dicembre 2003.

Data breach: l'art. 615-quinquies *(Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)* si pone indubbiamente come norma di sbarramento preventiva, rispetto ad un danneggiamento in senso lato di un sistema informatico o telematico ex art. 635-bis e ss., [235] così come l'art. 615-quater *(Abusiva acquisizione o diffusione di codici d'accesso ad un sistema informatico o telematico)* si poneva quale anticipazione della soglia di tutela rispetto alla vera e propria fattispecie di accesso abusivo ad un sistema informatico ex art. 615-ter. [236]

Come si è anticipato, la tutela sanzionatoria *de quo* è rafforzata dalla apposita fattispecie incriminatrice successiva (l'art. 635-ter) che sanziona i medesimi fatti di danneggiamento riguardanti informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità: ciò che rileva, in sostanza, è l'utilità sociale dell'oggetto dell'aggressione, per le gravi conseguenze lesive che potrebbero derivarne per la salvaguardia degli interessi pubblici.

Quest'ultima norma si presenta peraltro di più ampia portata, nel suo primo comma infatti costruisce il reato quale reato di pericolo, attraverso la previsione della punibilità delle condotte *"dirette a"* distruggere, deteriorare, etc. le informazioni, i dati ed i programmi ad alta sensibilità collettiva. La concreta realizzazione dello scopo (l'effettiva distruzione, cancellazione, etc.) integra infatti una diversa ed autonoma ipotesi di danno, prevista e sanzionata più pesantemente al secondo comma del medesimo articolo.

Sono previste infine le medesime circostanze aggravanti sopra esaminate a proposito dell'art 635-bis, per cui si avrà un ulteriore aggravamento di pena qualora il fatto incriminato sia commesso con violenza o con minaccia alla persona oppure con abuso della qualità di operatore di sistema.

---

235 Ciò non esclude, ovviamente, la configurabilità del tentativo di danneggiamento, a meno che la condotta non coincida con quella prevista dall'art 615-quinquies c.p., nel qual caso, per il principio di specialità, dovrà trovare applicazione solo il reato previsto da tale norma che, appunto, costituisce una anticipazione della soglia di tutela.

236 Rispetto alla condotta di accesso abusivo si noti come sia ritenuto ammissibile il concorso di tale reato con quello di danneggiamento informatico (art 635-bis) nelle sole ipotesi in cui l'accesso abusivo non sia limitato al tempo strettamente necessario per danneggiare: quando infatti l'accesso coincide o è strettamente finalizzato alla condotta vandalica è da ritenere che il reato in questione sia assorbito nel più grave reato ex art. 635-bis.

Per provvedere adeguatamente alle indicazioni della Convenzione di Budapest, il sistema sanzionatorio è stato completato con l'introduzione di due fattispecie incriminatrici dirette a punire le condotte di danneggiamento che abbiano ad oggetto non singoli documenti, dati o programmi, bensì il funzionamento di un intero sistema informatico o telematico. [237]

Si tratta invero dei nuovi articoli 635-quater e 635-quinquies c.p., redatti in modo speculare rispetto alle corrispondenti ipotesi di reato, sopra analizzate, proprie degli articoli 635-bis e 635.ter c.p.

Oltre alle molteplici condotte di danneggiamento, a cui si rimanda, già previste dall'art 635-bis, [238] il delitto in esame, ex art. 635-quater, può esser commesso altresì mediante *"l'introduzione o trasmissione di dati, informazioni o programmi"*: ed è quest'ultima l'ipotesi in cui il reato si veda commesso tramite la diffusione di *malware*, atti a cagionare proprio uno degli eventi di distruzione, danneggiamento, inservibilità od ostacolo al funzionamento di un intero sistema (agile viene qui il richiamo agli attacchi di tipo ransomware sopra descritti).

Ancora, risulta sanzionato non solo il rendere *"in tutto o in parte inservibile il determinato sistema informatico",* ma anche l'averne parimenti "ostacolato gravemente" il funzionamento, trattasi quest'ultima di una condotta di non sempre facile apprezzabilità, essendo che richiede una valutazione prognostica circa gli esiti di una condotta che non ha concretamente prodotto in toto gli effetti dannosi cui era indirizzata. [239]

---

237 Quanto alla definizione di "sistema informatico", può essere utile ricordare l'art. 1 della Convenzione di Budapest, dove viene indicato come *"qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma, compiono l'elaborazione automatica di dati".*

238 Verranno sanzionate quindi, alternativamente, condotte quali la distruzione, il deterioramento, o l'inservibilità di un sistema telematico od informatico. Sebbene siano condotte diverse per caratteristiche morfologiche, si presentano accumunate dall'eguale attitudine a produrre un medesimo risultato, che è poi l'evento tipico della fattispecie: l'alterazione funzionale o strutturale della cosa, ovvero un suo deterioramento, purché sia di un certa consistenza ed evidenza.

239 La previsione si spiega in ragione delle indicazioni contenute nella Convenzione di Budapest, dove l'attentato all'integrità di un sistema informatico viene costruito attribuendosi rilievo ad ogni condotta che si sostanzi in un *"serio pericolo"* al funzionamento del sistema stesso, anche laddove questo non venga in toto danneggiato e reso inservibile.

Va infine evidenziato come l'art. 635-quinquies sia costruito in modo identico rispetto all'635-ter, con l'obiettivo di rafforzare la tutela sanzionatoria indirizzata agli stessi fatti di danneggiamento laddove abbiano ad oggetto sistemi informatici o telematici di pubblica utilità, nonché parimenti si presenta costruita quale fattispecie di pericolo laddove prevede che vengano puniti gli atti idonei ed univoci "diretti a" distruggere, danneggiare, render inservibile od ostacolare gravemente il funzionamento del sistema.

Da ultimo, trattando di attacchi ransomware, non si può prescindere dal prendere in considerazione anche il delitto di estorsione ex art. 629 c.p., consistente nella costrizione di qualcuno mediante violenza o minaccia a fare od omettere qualche cosa, col fine di procurare a sé o ad altri un ingiusto profitto, con l'altrui danno, per cui si sarebbe ivi di fronte ad un estorsione di tipo telematico, in cui la tecnologia rappresenterebbe il mezzo dell'azione del reo.

Si è visto come la condotta realizzata tramite ransomware sia bifasica: ad un attacco alle risorse informatiche (consistente nel criptare i file memorizzati, impedendo l'accesso al sistema, ed ostacolandone il riavvio) segue proprio una minaccia telematica, ossia una prospettazione di una ingiustizia futura, accompagnata da una richiesta di pagamento: la somma di denaro dovrà esser corrisposta entro termini perentori per ottenere la chiave di decrittazione (e per impedire che i dati stessi vengano, laddove esfiltrati, resi pubblici).

La nozione di "violenza informatica" è peraltro ricavabile dall'art. 392, comma 3 c.p. dove si ricava come si abbia violenza sulle cose anche qualora *"un programma informatico venga alterato, modificato o cancellato, in tutto o in parte, ovvero venga impedito o turbato il funzionamento di un sistema informatico o telematico"*, dunque allorché il malware abbia compromesso il sistema (ad esempio disattivandone le opzioni di avvio) la suddetta nozione di violenza informatica sarebbe soddisfatta, così come sarebbe configurabile la fattispecie della cyber-estorsione.

Si noti ancora come l'articolo 629 c.p. si caratterizzi quale delitto contro il patrimonio, con cooperazione involontaria della vittima, nonché quale reato plurioffensivo (in quanto posto a tutela tanto del patrimonio, quanto della libertà morale del

soggetto passivo): in tal senso anche nell'estorsione a mezzo ransomware si può scorgere la compromissione di una serie di beni giuridici, connessi alle tecnologie dell'informazione, quali la riservatezza e la sicurezza informatica, la libertà e la confidenzialità delle comunicazioni, o il concetto stesso di privacy informatica.

È ormai chiarito infine come il delitto di estorsione si consumi nel momento e nel luogo in cui si realizzano gli eventi del profitto ingiusto, con l'altrui danno, senza dubbio però in una cyber *extortion* a mezzo ransomware risulta di difficile individuazione il momento, nonché il luogo d'effettivo conseguimento del profitto (venendo il riscatto solitamente versato attraverso metodi non propriamente tracciabili), pertanto per una loro corretta individuazione, connessa a quella circa l'autorità giudicante competente si dovrà ricorrere ai criteri supplettivi, previsti ex art. 9 c.p.p.

4.9 Cybercrime as a Service: caso LockBit

La creazione di *malicious software* (o malware), quali sono i ransomware, è diventata col tempo una vera e propria industria sotterranea, un business competitivo ed in continua evoluzione, in grado di adattarsi a quelli che sono i repentini cambiamenti socio-economici mondiali. Si voglia pertanto di seguito andare a tratteggiare uno dei suoi più recenti protagonisti, ossia il cyber-gruppo criminale denominato come *LockBit*.

È invero solo negli ultimi anni che la sopradetta gang criminale, originaria dell'Europa orientale, ha incominciato ad affermarsi come membro d'élite della comunità underground, dacché contraddistinta da competenze tecniche di rilevo e da un modello di business innovativo in breve tempo è riuscita ad imporre il proprio prodotto come standard di riferimento nel complesso panorama delle minacce ransomware. Così le parole di commento di Toby Lewis, *Global Head of Threat Analysis* di Darktrace, società di IT anglo-americana, specializzata nel settore della cyber-difesa: *"LockBit, l'ormai nota gang ransomware-as-a-service, sta attraversando una fase di rapida crescita, con una adesione in continuo aumento*

ed un processo che risulta amplificato anche a seguito della caduta del gruppo Conti. LockBit dispone di un modello di business decisamente sofisticato, che ha permesso solamente quest'anno di attaccare già diverse organizzazioni europee: dal Dipartimento di Giustizia francese, ai gestori di pensioni tedesche Heubeck AG."

In dettaglio il nuovo software malevolo configurato e presentato al mondo dalla cyber-crew (denominato, in omonimia, "ransomware LockBit",) appartiene alla sottoclasse di nuova generazione dei *crypto-virus,* intendendosi quei virus informatici progettati per criptare i file presenti in un sistema, col fine di chiedere in seguito alla vittima un riscatto finanziario in cambio dell'ottenimento della chiave di decifratura, quale unico metodo possibile per rientrare in possesso dei propri dati. [240] Come più volte ribadito, gli obiettivi in maggior misura esposti a tale tipologia di attacco sono proprio quei soggetti maggiormente suscettibili, nonché danneggiabili dalla interruzione dei propri sistemi, così da essere di conseguenza anche i più propensi, avendo i fondi sufficienti, al versamento del riscatto monetario. Pertanto, si sarà intuito, target vulnerabili risultano essere le aziende di grandi dimensioni, dagli istituti finanziari a quelli sanitari (d'altronde nel previo capitolo già si è avuto modo di accennare al gruppo LockBit trattando proprio dell'attacco informatico di tipo ransomware indirizzato all'Ulss Euganea di Padova dell'anno 2021).

Ciò che più contraddistingue il gruppo criminale de quo è l'adozione dello specifico modello di business definito come *"Ransomware-as-a-Service"* (lett. "ransomware distribuito come servizio") tramite cui un gruppo criminale affiliato più piccolo, con verosimilmente meno risorse interne, affitterà il ransomware "pronto all'uso" di un cyber-gruppo più grande per realizzare i propri attacchi. [241]

È una modalità di impresa curiosamente speculare al modo legittimo in cui semplici sviluppatori di *software* distribuiscono i prodotti SaaS *(Software-as-a-servi-*

---

240 S. S. Anandrao,"Cryptovirology: "Virus approach", in *International Journal of Network Security and Its Applications* (IJNSA), Vol. 3, N. 4, July 2011, pp. 33-46.

241 P. H. Meland, Y. F. Bayoumy, G. Sindre, "The ransomware-as-a-Service economy within the darknet" in *Computers and Security*, Vol. 92, 29 February 2020, pp.1-8.

ce) nel mercato lecito, con la ovvia differenza che i Kit RaaS (facilmente reperibili grazie alla loro larga pubblicizzazione sul dark web), consentiranno ad attori malintenzionati, manchevoli di capacità tecniche o di tempo per sviluppare le proprie varianti ramsomware, di essere comunque operativi in modo rapido e conveniente.

Il meccanismo è dunque lineare: il team di sviluppatori di LockBit fornirà le proprie "armi" informatiche (non solo *ransomware taylor-made*, ma anche tools di post-intrusione, liste di accessi etc.) ai propri clienti che le impiegheranno per portare a compimento specifici attacchi, ricevendo in seguito come corrispettivo dello scambio una quota del riscatto ottenuto (tipicamente attorno al 20-30%, in aggiunta alla *malware creation fee*).[242]

Si provino ora a riassumere le fasi di un attacco operato tramite LockBit:[243]

a. ***Exploit dei punti deboli di una rete:*** i gruppi criminali affiliati selezionano i loro potenziali obiettivi e ne "bucano" il sistema, facendo affidamento sui metodi più svariati, quali le tattiche di social engineering (si pensi al *phishing*), la scansione massiva delle vulnerabilità, o semplicemente acquistando *nell'underground digitale* accessi RDP (Remote Desktop Protocol) già compromessi. Peraltro non è raro che siano proprio gli stessi membri del gruppo LockBit a specializzarsi nella acquisizione illecita di credenziali di accesso per rivenderle sul web ricavandone in tal modo ulteriore profitto.

b. ***Infiltrazione:*** prima ancora della crittografia LockBit intraprenderà in modo indipendente tutte le azioni di preparazione alla configurazione dell'attacco: si pensi alla disabilitazione dei programmi di sicurezza o di qualsiasi altra infrastruttura che potrebbe consentire il ripristino del sistema. L'obiettivo dell'infiltrazione consiste nel rendere ir-

242 *Ibidem*.

243 E. De Lucia, "L'analisi tecnica: LockBit, chi è e come agisce la gang del ransomware", in *Cybersecurity360*, testata editoriale di Digital360, 12 Agosto 2021.

realizzabile un ripristino automatico del sistema o ad ogni modo di rallentarlo a sufficienza cosicché l'unica soluzione pratica per la vittima sia quella di arrendersi al pagamento del riscatto.

c. ***Esecuzione:*** una volta preparata la rete per la mobilitazione completa di LockBit, il malware stesso avvia in automatico la sua propagazione verso qualsiasi dispositivo che sia in grado di raggiungere. Ciò che rende particolare LockBit è proprio il fatto di essere un ransomware operante in modalità SAR *(Semi-Automated Ransomware),* dotato cioè della capacità di diffondersi e autopropagarsi in autonomia: dopo che l'attacco ha infettato un singolo host, può difatti trovare altri host accessibili, connetterli a quelli infetti a condividere l'infezione tramite uno script, il tutto interamente senza bisogno dell'intervento umano.

d. ***Trattativa:*** così si giunge alla vera e propria fase di criptaggio, tramite cui si pone un "blocco" su tutti i file del sistema, rilasciando un semplice file di testo contenente la sopradetta richiesta di riscatto: la vittima è invitata a prendere contatto con l'attaccante al fine di procurarsi il "*decryptor*" necessario al recupero di file e documenti resi indisponibili. Ovvio è che a questo punto gli attaccanti potranno utilizzare svariati approcci psicologici per spingere e coartare la vittima al pagamento (si pensi alla classica imposizione di un *countdown* unito alla minaccia di render pubblici tutti i dati esfiltrati).

Quale regola d'oro del mondo digitale tutto, si ponga in rilievo l'importanza della mitigazione del rischio, come altresì dell'adozione di misure precauzionali atte a garantire che una data organizzazione sia resiliente ad eventuali attacchi informatici sin dall'inizio.

Si elenchino perciò, a fini chiarificatori, alcune tecniche preventive utili a proteggersi specificatamente da quella che è la minaccia LockBit, fra cui: [244]

a. realizzare *backup* periodicamente aggiornati, mantenendo così sempre una copia crittografata dei dati *offline*;

b. operare frequenti *check-up* dei sistemi per rilevare e rimuovere account obsoleti, inutilizzati e mai disattivati in quanto potenziali punti deboli del sistema;

c. implementare l'impiego di password sicure, complesse ed univoche (si è già potuto notare come molte delle violazioni si verifichino a causa di *default password* mai cambiate o sufficientemente semplici da rilevare tramite strumenti basati su algoritmi di analisi);

d. impostare l'autenticazione a più fattori [245] ove possibile, andando così a sommare più livelli di accesso (si pensi ad esempio alle potenzialità del riconoscimento biometrico);

e. limitare il più possibile la concessione di privilegi di amministrazione, applicando strategie di accesso *Zero-Trust* [246] in modo da impedire a potenziali minacce di passare inosservate;

f. applicare modelli di *network segmentation,* suddividendo cioè la rete in diverse sottoreti, ossia unità più piccole e gestibili, ciascuna dotata di controlli e servizi sicurezza unici, limitando in tal modo la diffusione laterale di un eventuale malware e riducendo al minimo la superficie di attacco;

---

244 FBI, *Indicators of Compromise associated with LockBit* 2.0, FBI Cyber division, 4 February 2022.

245 Per *Multi-Factor Authentication* o MFA si intende un metodo di autenticazione sicuro che chiede agli utenti di dimostrare la propria identità fornendo due o più prove (o fattori) nel momento stesso in cui eseguono l'accesso (ad esempio oltre alla password agli utenti potrebbe esser richiesto di inserire un codice inviato tramite e-mail).

246 Si ripeta come un approccio di tipo Zero trust (letteralmente "nessuna fiducia"), sia basato sull'assunto che nessun utente deve intrinsecamente esser ritenuto attendibile, per cui dovrà essere costantemente autorizzato prima di poter accedere ad una rete, ciò permette di scovare azioni sospette anche laddove queste siano riconducibile ad una utenza considerata al di sopra di ogni sospetto (come quella di un *admin*).

g. verificare se l'organizzazione utilizzi dispositivi e/o servizi per l'accesso remoto e risolvere eventuali loro vulnerabilità e debolezze segnalate.

Si transiti a seguire verso l'analisi di un'ultima tipologia di cyberminacce, che bramano come target non più un sistema informatico nel suo complesso, quanto un dispositivo, strumento od apparecchiatura medicali, col preciso fine di impattare sulla disponibilità del servizio che questi supportano, quanto sulla riservatezza dei dati raccolti, nonché altresì sulla sicurezza del paziente stesso che ne stia facendo uso.

C. CYBER-INTRUSIONI IN DISPOSITIVI MEDICALI

4.10 La tecnologia al servizio della salute

È fuor di dubbio che l'intelligenza artificiale abbia ottenuto grandi successi a partire dal primo decennio del XXI secolo: si è difatti assistito alla diffusione di robot e sistemi di IA nei settori più disparati, quali la difesa militare, il settore aereospaziale, i sistemi bancari, i trasporti aerei e terrestri, i processi industriali e ancora, per ciò che ivi interessa, nella sanità. [247]

Già nel 2013, l'agenda strategica di ricerca per la robotica in Europa [248] segnalava come tali tecnologie sarebbero diventate dominanti nel corso del decennio successivo, influenzando fortemente ogni aspetto della vita pubblica e privata degli individui ed accrescendo così le occasioni di interazione tra esseri umani e sistemi d'intelligenza artificiale.

Addentrando la trattazione nell'ambito sanitario, si evidenzi innanzitutto come la robotica e i sistemi di IA siano progettati e sviluppati per svolgere molteplici funzioni: coadiuvare il lavoro dei medici estendendo le possibilità di intervento nelle operazioni chirurgiche a distanza, dare supporto nei processi decisionali in ambito diagnostico e terapeutico, assistere i pazienti nelle attività di riabilitazione, supportarli nei programmi di prevenzione, finanche a poterne migliorare le capacità fisiche (si pensi al settore delle protesi robotiche). [249]

Data l'enorme vastità e diversità delle tecnologie e dei sistemi di IA in ambito sanitario, si tenti primariamente di darne un, seppur generico, ordine tramite clas-

---

247 F. Lagioia, *L'intelligenza artificiale in sanità: un'analisi giuridica*, Giappichelli Editore, Torino, 2020, pp. 1-5.

248 euRobotics aisbl (Association Internationale Sans But Lucratif), *Strategic agenda for Robotics* in Europe 2014-2020, 11 Ottobre 2013.

249 Butter M, Rensma A., et al., Robotics for *ealthcare*: Final report, European Commission, DG information society, 3 Ottobre 2008.

sificazione delle macro aree maggiormente toccate dall'innovazione tecnologica *de quo*: l'area clinica, l'area riabilitativa e quella assistenziale. [250]

a. L'area clinica ricomprende tutto ciò che più propriamente afferisce ai processi di cura dei pazienti (ossia diagnosi, trattamenti, interventi chirurgici, nonché assistenza sanitaria d'emergenza).
Le tecnologie, gestite dal personale clinico qualificato, che afferiscono a tale area possono esser identificate in sistemi ed applicazioni che consentono interventi a distanza, sistemi di supporto alle decisioni diagnostiche e terapeutiche, ed ancora sistemi che migliorano tanto le abilità chirurgiche, quanto l'efficacia degli interventi stessi.

b. L'area riabilitativa invece ricomprende un vasta gamma di applicazioni per l'assistenza di pazienti affetti da disabilità fisiche e/o mentali (si pensi ai disturbi neurologici, alle lesioni parziali del midollo spinale, come anche alle patologie legate all'invecchiamento).
In tale area sarà principalmente la robotica a supportare i suddetti programmi riabilitativi, così da favorire il recupero delle funzionalità parzialmente compromesse o da agire in sostituzione di quelle perdute.

c. L'area assistenziale infine ricomprende quei sistemi la cui funzione primaria è fornire, per l'appunto, assistenza a pazienti ed operatori sanitari, in contesti ospedalieri e in strutture di assistenza specialistica. In tale area saranno impiegate tecnologie per lo svolgimento di attività di routine di natura logistica (dalla cura personale, alla fornitura di farmaci), nonché tutto ciò che concerne il monitoraggio a distanza dei pazienti, o propriamente i video-consulti virtuali medico-paziente.

---

250 Lagioia F, "Intelligenza artificiale e robotica in sanità" in Lagioia F. (a cura di) *L'intelligenza artificiale in sanità: un'analisi giuridica,* Giappichelli Editore, Torino, 2020, pp. 7-42.

Date tali premesse, si passi ora a considerare la normativa europea di settore in tema di dispositivi medici, così da poterne avere una corretta ed attuale qualificazione giuridica. A tenore infatti dell'art. 2, comma 1, del nuovo Regolamento UE 2017/745, rientra nella definizione di dispositivo medico: [251]

"[...] qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche:

- *Diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie;*
- *Diagnosi, monitoraggio, trattamento, attenuazione, o compensazione di una lesione o di una disabilità;*
- *Studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico;*
- *Fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati;*
- *Dispositivi per il controllo del concepimento o il supporto al concepimento;*
- *I prodotti specificatamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi medici; "*

Da questo punto vista , il suddetto Regolamento Ue 2017/745 non ha introdotto modifiche sostanziali alla definizione di dispositivo medico, rispetto alla normativa precedente. Le precisazioni sulle finalità mediche di un dispositivo erano peraltro già contenute nelle linee guida comunitarie MEDDEV 2.2.1 ex art. 1 lett.

---

251 Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio, per una integrale consultazione si rimanda al sito internet https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex:32017R0745.

b) secondo cui *"la finalità medica è assegnata a un prodotto dal fabbricante. Il fabbricante ne determina la finalità mediante l'etichettatura, le istruzioni d'uso e il materiale informativo del dispositivo"*. [252]

Ancora, l'allegato VIII del soprarichiamato Regolamento Ue 2017/745 identifica differenti classi di rischio relative ai dispositivi medici, sulla base di tre criteri principali, di seguito elencati: [253]

a. Durata d'utilizzo del dispositivo e contatto con il corpo: distinguibile in temporaneo, a breve termine e a lungo termine;

b. Invasività del dispositivo: si possono infatti differenziare dispositivi non invasivi (ossia non penetranti fisicamente il paziente), invasivi negli orifizi del corpo, invasivi chirurgici, ed impiantabili.

c. Dipendenza da una fonte di energia: distinguendo così in dispositivi non attivi, attivi terapeutici e attivi diagnostici. Si noti come un dispositivo si definisca attivo qualora dipenda, per poter funzionare da una fonte di energia diversa da quella generata direttamente dal corpo o dalla forza di gravità, e operi mediante un processo di conversione di tale energia.

Sulla base dei suddetti criteri dunque i dispositivi medici vengono classificati in quattro classi di rischio, al cui vertice si posizioneranno tutti i dispositivi impiantabili per il supporto vitale (si pensi ad un pacemaker o ai ventilatori polmonari), proprio a causa dei maggiori rischi che potenzialmente possono comportare, andando ad interagire con le funzioni di organi vitali. Si sono volute fornire le previe, seppur coincise, delucidazioni in materia di dispositivi medicali al fine di arrivare all'argomento che più qui interessa: ossia il rischio informatico, nella fattispecie identificabile soprattutto in un pericolo di manipolazione dall'esterno dei dispositivi (c.d. hackeraggio).

---

252 European commission, DG enterprise, *Guidelines to the application of: the council directive 90/385/EEC on active implantable medical devices*, the council directive 93/42/EEC on medical devices, Meddev 2.1.1, April 1994.

253 F. Lagioia, opera cit. *supra* a nota 247, pp. 86-89.

La direzione crescente verso la messa in rete e la connettività dei dispositivi medicali (non a caso, si parla di IoMT, ossia *Internet of Medical Things*), è associata infatti sempre più ad un corrispondente aumento delle vulnerabilità di tali dispositivi nei confronti di *malware* informatici e violazioni, che possono condurre tanto a malfunzionamenti del dispositivo, quanto ad interruzioni degli stessi servizi sanitari. [254]

Si fornisca, un possibile esempio di *hacking* relativo ad un macchinario per la risonanza magnetica (MRI), riportando nella tabella sottostante (Tab. 4.4) ipotetiche condotte cyber-criminali, a cui poter associare specifici risultati malevoli. [255]

ATTIVITÀ HACKER	POSSIBILI RISULTATI
Aumentare la potenza e l'intensità del campo magnetico	Potenziale riscaldamento dei tessuti ed ustioni per il paziente. Eventuale danneggiamento del macchinario
Disattivare gli allarmi	Il personale medico-sanitario non sarà a conoscenza delle condizioni di pericolo
Disattivare il macchinario, crittografare i file interni e/o interferire con il suo funzionamento	Richiesta di un riscatto per rispristinarne il corretto funzionamento
Riavvio della macchina	Eliminazione delle impostazioni di configurazione
Far sì che la macchina associ il file di un paziente all'immagine di un altro paziente	La diagnosi verrà consegnata al paziente errato

Tab 4.4 Condotte di hacking indirizzate ad un macchinario MRI e dirette possibili conseguenze.

254 ECRI institute, "Top 10 Health technology Hazards for 2015", in *Health Devices,* November 2014, pp. 26-29.

255 Rocchi W., "Cyber security nel settore sanitario, a rischio apparecchiature mediche e dati riservati: lo scenario", in *Cybersecurity360*, testata editoriale di Digital360, 5 Maggio 2020.

Da qui si ricavi come la possibilità per un hacker di accedere a dispositivi medici possa avere un impatto tanto sulla disponibilità del servizio che il dispositivo supporta (ad esempio alterandone le rilevazioni), quanto sulla riservatezza dei dati raccolti, nonché addirittura sulla sicurezza del paziente stesso che ne stia facendo uso (si pensi ai possibili danni per i tessuti biologici od all'area cui il device stesso risulta connesso).

Di seguito si vorrà approfondire.

4.11 Hacking medicale

Si voglia prendere ora in considerazione il Rapporto sulla sicurezza dei dispositivi medici IoT e IoMT, condotto dalla società di sicurezza informatica Cynerio, dal titolo *"State of Healthcare Iot Device Security Report 2022",* quale studio condotto su di un campione di 10 milioni di dispositivi medici connessi (anche *connected medical devices*), distribuiti in oltre 300 ospedali, cliniche e altre strutture sanitarie in tutto il globo.[256]

Dal suddetto report emerge un quadro allarmante: negli ambienti sanitari invero le minacce alla sicurezza relative ai dispositivi medicali risultano essere gravemente sottovalutate, nonostante emerga in maniera parimenti evidente come la sicurezza digitale e quella dei pazienti siano profondamente connesse, dal momento che è proprio dalla protezione degli stessi dispositivi che deriva la salvaguardia di valori quali la salute, l'integrità ed il benessere degli individui.[257]

Si elenchino di seguito i risultati chiave emergenti dal rapporto:

a. Il 53% dei dispositivi medici connessi ad Internet risulta affetto da almeno una vulnerabilità nota. Se attaccati, potranno im-

---

256 Cynerio, *The State of Healthcare IoT Device Security 2022,* Cynerio, 2022, reperibile integralmente al sito internet https://www.cynerio.com/landing-pages/the-state-of-healthcare-iot-device-security-2022.

257 F. Del Gaudio, "La sicurezza dei dispositivi medici ospedalieri connessi a rischio hacker", in *Filodiritto: quotidiano di diritto, cultura e società,* 3 Maggio 2022.

pattare tanto sulla sicurezza dei pazienti, quanto sulla disponibilità dei servizi, come anche sulla riservatezza dei dati elaborati. Ancora, circa un terzo dei *bedside healthcare devices,* dai quali i pazienti, si capirà, dipendono maggiormente, presentano un rischio di sicurezza identificato come critico. Ebbene, da tali dati si deduca come alle strutture sanitarie manchi verosimilmente una visione ad ampio raggio circa tutti i possibili rischi informatici impattanti sui propri dispositivi, nonché sulle conseguenze disastrose che ne potrebbero derivare.

b. Nello specifico poi, i dispositivi connessi più comuni negli ambienti ospedalieri risultano essere le pompe infusionali [258] (rappresentando infatti il 12% di tutti i *connected devices,* ed il 38% dei dispositivi IoMT rilevati da Cynerio). Queste ultime sono parimenti i dispositivi detentori della più alta quota di rischio, il 73% di esse infatti presenta un qualche tipo di vulnerabilità che metterebbe a repentaglio la sicurezza dei pazienti laddove venisse sfruttata da un avversario malevolo.

c. Ulteriore aspetto sconfortante di tale panorama è il fatto che buona parte delle anzidette vulnerabilità sia dovuta proprio alla mancanza di basilari nozioni di sicurezza informatica.
Il rapporto infatti evidenzia come i dispositivi siano spesso dotati di *default passwords* [259] che restano invariate nel tempo e che gli stessi aggressori possono ottenere agilmente da manuali reperibili online, più precisamente circa il 21% dei dispositivi risulta protetto, per l'appunto, da credenziali deboli o predefinite.
Ancora, una buona parte delle vulnerabilità rilevate è dovuta

---

258 La pompa infusionale è un dispositivo elettronico, per la somministrazione di farmaci o prodotti medicali, che permette di infondere la terapia endovenosa o enterale in maniera particolarmente precisa (tenendo sotto controllo le gocce infuse), garantendo somministrazione e velocità esatte.

259 Quando un dispositivo richiede un nome utente e/o una password per accedere, di solito viene fornita una *default password* che consente, per l'appunto, l'accesso durante la configurazione inziale. I produttori di tali apparecchiature in genere utilizzano password basilari (quali admin o password) nell'aspettativa poi che gli utenti cambino in seguito le credenziali. Il nome utente e la password predefiniti si trovano solitamente nei manuali d'istruzione, comuni a tutti i dispositivi.

> all''utilizzo di software obsoleti o non aggiornati. Nel rapporto si sottolinea infatti come dispositivi basati su versioni precedenti a Windows 10 siano largamente impiegati nei reparti di radiologia, neurologia, chirurgia, farmacologia ed oncologia, facilitandone l'eventuale compromissione. Da ciò si ricavi come alcune delle vulnerabilità più comuni potrebbero esser affrontate facilmente, laddove ci si dotasse di strumenti opportuni e di una cyber cultura adeguata.

Queste le parole di commento di Daniel Brodie, CTO [260] e co-fondatore di Cynerio *"L'assistenza sanitaria è uno degli obiettivi principali per gli attacchi informatici e, nonostante i continui investimenti nella sicurezza informatica, permangono vulnerabilità critiche in molti dei dispositivi medici su cui gli ospedali fanno affidamento per la cura dei pazienti. [...] Gli ospedali e i sistemi sanitari hanno bisogno di soluzioni avanzate che riducano i rischi e che consentano loro di combattere gli attacchi informatici e, come fornitori di sicurezza dei dispositivi medici, è tempo di farsi avanti"*.

Nel prosieguo della trattazione si propongano due esemplificazioni, inerenti a dispositivi medicali risultati concretamente a rischio hacker, più precisamente si tratterà di pompe per l'insulina e di dispositivi *pacemakers*.

4.11.1 Dispositivi IoMT a rischio: i casi

Si premetta innanzitutto come ad oggi siano indubbiamente aumentate le apparecchiature medicali che sfruttano software e sistemi di comunicazione *wireless*, col fine di permettere a medici (o agli stessi pazienti) di ricevere i dati biomedici in tempo reale, così da poter monitorare agilmente lo stato di salute individuale. Per il primo caso occorre risalire al 9 Agosto 2018, data in cui *Medtronic*, azienda statunitense, e leader globale nel settore

260 Per CTO si intenda *Chief technology Officer.*

delle tecnologie biomediche, emise un comunicato urgente relativo ai controller *MiniMed MMT-500 e MMT-503 (Fig. 4.5)*, ossia telecomandi progettati per comunicare con i rispettivi microinfusori di insulina, così da consentire ai pazienti diabetici di programmare l'erogazione di una predeterminata quantità di bolo insulinico.[261] Col suddetto avviso, si è voluta informare la propria clientela in merito a sopraggiunti rischi di sicurezza informatica: come è immaginabile, gli anzidetti telecomandi comunicano da remoto con i microinfusori di insulina, utilizzando un segnale *wireless* in radiofrequenza (RS), ed è proprio questa caratteristica a determinare il sorgere di specifiche vulnerabilità.

The following list shows the Medtronic remote controller and compatible Medtronic insulin pump(s) that are vulnerable to this issue. Medtronic will notify users whose records are on file.

Remote controller	Model Number Location	Compatible Insulin pump(s)
 MiniMed™ remote controller **MMT-500**	 The model # is behind the remote under the barcode	Medtronic MiniMed™ 508 pump
 MiniMed™ remote controller **MMT-503**	 The model # is behind the remote under the barcode	MiniMed™ Paradigm™ 511 pump MiniMed™ Paradigm™ 512/712 pumps MiniMed™ Paradigm™ 515/715 pumps MiniMed™ Paradigm™ 522/722 pumps MiniMed™ Paradigm™ 523/723 pumps MiniMed™ Paradigm™ 523(K)/723(K) pumps MiniMed™ 530G 551/751

Fig 4.5 Tabella riportante i telecomandi Medtronic, con i relativi microinfusori di insulina compatibili, interessati dalla vulnerabilità informatica. Fonte: Medtronic, Urgent Field Safety Notice: MiniMed remote controller (MMT-500 or MMT-503), August 2018.

261 Medtronic, *Urgent Field Safety Notice: MiniMed remote controller* (MMT-500 or MMT-503), August 2018, per una integrale consultazione, in traduzione, si rimanda al sito internet https://www.salute.gov.it/imgs/C_17_AvvisiSicurezza_8382_azione_itemAzione0_files_itemFiles0_fileAzione.pdf

Nel sopradetto comunicato, l'azienda prende coscienza di come un individuo non autorizzato, purché si trovi nelle immediate vicinanze di un microinfusore, potrebbe potenzialmente copiare i segnali *wireless* inviati legittimamente dall'utente (nel momento in cui quest'ultimo stia utilizzando il controller per l'erogazione del bolo) per poi riprodurli in successivi momenti, con l'intento o di forzare sovradosaggi di insulina, eventualmente provocando nei pazienti diabetici crisi ipoglicemiche, oppure di bloccarne del tutto la stessa erogazione, provocando viceversa eventuali condizioni di iperglicemia o di chetoacidosi diabetica, ad ogni modo, si capisce, mettendo a serio rischio lo stato di salute degli individui.

L'azienda risulta ad ogni modo intenzionata a ribadire come l'anzidetta comunicazione sia stata rilasciata a scopo unicamente informativo, non venendo esplicitamente richiesta infatti né la sostituzione, tantomeno la restituzione dei dispositivi (microinfusori e/o telecomandi), così infatti si legge nel prosieguo dell'avviso: *"Medtronic ha informato le autorità competenti preposte, diffuso un'informativa riguardante questo potenziale problema di sicurezza e informato i professionisti sanitari e gli utilizzatori in merito alle misure cautelative che possono esser adottate per proteggere la sicurezza del microinfusore. [...] La famiglia di microinfusori di insulina MiniMed Paradigm rimane sicura ed efficace nella gestione del diabete, Medtronic invita quindi gli utilizzatori a continuare la loro terapia come al solito e, in caso di dubbi, ad adottare a titolo cautelativo, le misure precedentemente indicate"*. [262]

Nonostante le sopradette rassicurazioni, il panorama dei microinfusori della Medtronic è ben presto peggiorato, e quelle che erano state delineate come potenziali vulnerabilità si sono tramutate in concreti rischi.

Solo pochi anni dopo infatti, precisamente nell'Ottobre del 2021, l'azienda de quo emette un nuovo richiamo urgente in cui si prende atto di come i rischi di hacke-

---

262 Fra i consigli elencati per proteggere la sicurezza del microinfusore infatti figurano: disattivare l'opzione "bolo rapido" quando non si ha effettivamente intenzione di usare l'opzione del bolo tramite il telecomando, o fare attenzione agli avvisi emessi dal microinfusore così da interrompere l'erogazione di qualsiasi bolo che non sia intenzionale, come anche non collegare il microinfusore a dispositivi terzi che non siano stati autorizzati da Medtronic.

raggio associati ai *cotroller MiniMed* superino di gran lunga i benefici di continuarne l'utilizzo. [263]

Così si legge nel nuovo comunicato: *"Gli utenti devono interrompere immediatamente l'utilizzo dei dispositivi, disconnettere il telecomando, disattivare le funzionalità di controllo da remoto e restituire il telecomando stesso alla Medtronic"*.

Ovvio è che si tratti pur sempre di attacchi di remota possibilità, per poter sabotare tali pompe di insulina è infatti necessario che si verifichino una serie di condizioni, quali: che il controllo da remoto della pompa sia stato attivato dall'utente, che il numero di serie (ID) del telecomando sia inserito nelle impostazioni dei microinfusore, che un individuo non autorizzato si trovi proprio nelle immediate vicinanze e con l'attrezzatura necessaria per copiarne i segnali in radiofrequenza attivati mentre lo stesso paziente stia effettuando l'erogazione di insulina, per poi successivamente trovarsi ancora nelle immediate vicinanze per inviare i comandi malevoli.

Purtuttavia da ciò si deduce anche come vi sia stata una falla in fase di sviluppo, progettazione e *design* del prodotto, ignorandone gli aspetti circa la sua cybersicurezza: se ad un attaccante infatti basta replicare un segnale in radiofrequenza significa che gli stessi segnali inviati alla pompa d'insulina non sono cifrati, ma in chiaro; e ciò è bastato per far tornare l'azienda sui propri passi, procedendo con un immediato ritiro dei dispositivi medicali.

Si voglia ora fornire un ulteriore esempio, prendendo in considerazione i dispositivi *pacemakers*, come anche i defibrillatori impiantabili. [264]

Parimenti in questo caso è possibile ipotizzare le conseguenze cliniche che delle malevoli interferenze potrebbero provocare: nel caso dei *pacemakers*, ad esem-

---

263 Medtronic, *Urgent Medical Device Recall: MiniMed remote controller (MMT-500 or MMT-503),* October 2021, per una sua integrale consultazione si rimanda al sito internet https://www.medtronicdiabetes.com/res/img/pdfs/MiniMed-Remote-Controller-FCA-Patient-Letter.pdf

264 Si evidenzi come un pacemaker abbia essenzialmente la funzione di ristabilire, inviando impulsi elettrici, un normale ritmo cardiaco (per i soggetti affetti da bradicardia), ed un defibrillatore impiantabile sia preposto viceversa a rilevare un battito cardiaco pericoloso, erogando, se necessario, una scarica salvavita che azzeri l'attività del cuore e che consenta il ripristino del regolare ritmo cardiaco.

pio, un hacker potrebbe manipolare gli input cardiaci, aumentandone notevolmente l'attività, o altresì impedirne proprio il corretto funzionamento scaricandone la batteria; viceversa nel caso dei defibrillatori impiantabili un soggetto non autorizzato potrebbe interrompere la comunicazione *wireless*, ostacolando la possibilità di tele-monitoraggio del paziente ed il conseguente rilevamento di situazioni pericolose (si pensi ad aritmie potenzialmente mortali), impedendone così l'intervento terapeutico salva-vita.

Così nel 2017 la FDA (ossia, *Food and Drug Administration*) statunitense ha emesso un richiamo urgente relativamente a circa 500.000 *pacemakers* prodotti dalla *San Jude Medical,* la quale è stata acquisita successivamente dalla Abbott, azienda globale nel campo *dell'health care.* [265]

Nonostante sia la stessa FDA a rassicurare che non vi siano casi registrati di danni ai pazienti correlati ad una condotta di manomissione da remoto dei suddetti dispositivi impiantabili, e nonostante lo stesso rischio di hacking rimanga relativamente basso (l'attaccante, anche in tal caso, dovrebbe trovarsi in stretta prossimità della propria vittima), l'Agenzia statunitense ha voluto espressamente confermare e rimarcare le vulnerabilità dei *pacemakers* ed i correlati rischi di sicurezza informatica, nonché di salute per i pazienti.

Nel caso de quo, il richiamo non ha tuttavia condotto alla rimozione e sostituzione dei *pacemakers* impiantati (procedura medica, si capirà, invasiva e potenzialmente pericolosa), ma ha visto una presa di posizione da parte della stessa società produttrice, la quale ha rilasciato un aggiornamento del firmware (ossia il sistema operativo dei dispositivi) applicabile da parte del personale medico specializzato, con l'obiettivo proprio di sopperire alle falle di sicurezza informatica sopravvenute.

Così infatti si legge nel successivo comunicato, indirizzato al personale medico-sanitario, emesso dalla Abbott: *"Vi avvisiamo della disponibilità di un nuovo firmware (una tipologia di software) per i pacemakers, atto a combattere il*

---

265 B. M. Kuehn, "Pacemaker recall highlights security concerns for implantable devices", in *Circulation-Cardiology News,* n. 138, 9 October 2018, pp. 1597-1598.

rischio di accesso non autorizzato ai nostri dispositivi che utilizzano segnali in radiofrequenza (RF). Suddetto aggiornamento fornisce un ulteriore livello di sicurezza contro l'accesso non autorizzato, così da ridurre ulteriormente le potenzialità di successo relative ad un cyber-attacco". [266]

Ancora una volta emerge chiaramente l'assoluta importanza di includere accorgimenti di sicurezza informatica già nella primordiale fase di progettazione dei medical devices: *"Provvedimenti che garantiscono la cybersicurezza devono essere adottati subito, fin dall'inizio, quando si cominciano a disegnare i software, [...] e richiedono la collaborazione di molti specialisti, inclusi esperti di software, di sicurezza e, ovviamente, medici",* così commenta D. Lakkireddy professore di Medicina *all'University of Kansas Hospital*.

È indubbio che dietro al dispositivo fisico medicale vi sia una infrastruttura complessa, organizzata, si potrebbe dire, su di un sistema multilivello, nonché plurisoggettivo: dai produttori delle componenti operanti a livello di hardware, a coloro che invece progettano il *software*, dalle imprese che forniscono servizi legati alla elaborazione dei dati (quali quelle svolgenti attività di data *analytics*), sino a *providers* dell'infrastruttura di rete e di connessione. [267]

I dispositivi medici software (DMS), così come i sistemi robotici e di AI, sono per lo più composti da una combinazione di *hardware* e *software*, e sono di conseguenza soggetti alla disciplina relativa alla responsabilità da prodotto difettoso, secondo quanto stabilito dalla Direttiva 85/374/CEE, [268] cui si affianca la disciplina del Regolamento (UE) 2017/745 in materia di dispositivi medici.

---

266 *"We are advising you of the availability of new pacemaker firmware (a type of software) that is intended to address the risk of unauthorized access to our pacemakers that utilize radio frequency (RF) communications. This firmware update provides an additional layer of security against unauthorized access to these devices that further reduces the potential for a successful cybersecurity attack".* Abbott, Important Cybersecurity Advisory: information about Cybersecurity Firmware Update, Abbott Society, 28 August 2017, per una integrale consultazione si rimanda al sito internet https://www.cardiovascular.abbott/content/dam/bss/divisionalsites/cv/pdf/reports/Pacemaker-Firmware-Update-Doctor-Letter-Aug2017-US.pdf

267 M. W. Monterossi, "Responsabilità civile e cybersicurezza nell'ecosistema dell'Internet delle cose", in *Giustiziacivile*, 2020, pp. 1-46.

268 Direttiva 85/374/CEE del Consiglio del 25 Luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, si rimanda al sito https://eur-lex.europa.eu/legal-content/IT/LSU/?uri=celex:31985L0374

Rimanendo ivi su una prospettiva di carattere generale, sul piano della responsabilità civile, si è a lungo discusso se fosse possibile configurare una sorta di responsabilità oggettiva in capo al produttore in tutti quei casi in cui i danni siano stati causati dallo stesso *software*, dato che il produttore risulta essere il soggetto che si trova nella posizione migliore per prevenire eventuali difetti del dispositivo, come anche per far fronte ad eventuali rischi connessi agli attacchi informatici, adottando le adeguate misure tecniche di protezione del dispositivo, nelle varie fasi di *design*, fabbricazione ed installazione. [269]

Tuttavia è fuor di dubbio che le caratteristiche delle nuove tecnologie, come anche la complessità dei ruoli coinvolti nel loro sviluppo, rendano spesso ardua l'allocazione di responsabilità: si pensi ad esempio alla *development risk defence,* che permette al produttore di evitare l'attribuzione di responsabilità laddove lo stato delle conoscenze tecnico-scientifiche, al momento della messa in circolazione del prodotto, sia tale da non consentire la scoperta e l'individuazione del difetto. Ovvio è che a fronte delle caratteristiche dei moderni sistemi di intelligenza artificiale, tale limitazione di responsabilità rischierebbe di espandersi in modo incontrollato, aumentando i rischi di vuoti di responsabilità.

Va qui inoltre ricordato anche come sia prevista una mitigazione della responsabilità del produttore tutte le volte in cui l'utente utilizzi in maniera errata od impropria il *software*, agendo così con negligenza (in tal caso si utilizza la nozione di negligenza contributiva). [270]

Non è infatti un caso che il Parlamento ed il Consiglio dell'Unione Europea abbiano voluto evidenziare come: *"La cybersicurezza, nel nuovo sistema Iot, richieda la partecipazione attiva degli utenti finali, chiamati a curare l'igiene informatica dei propri dispositivi, attraverso semplici misure di routine che possano contribuire a ridurre il rischio di danni a sé o ad altri"*. [271]

---

269 E. Macrì. opera cit. *supra* a nota 116, pp. 20-21.

270 F. Lagioia, op. citata *supra* a nota 247, pp. 95-99.

271 M. W. Monterossi, op. citata *supra* a nota 267, p. 25.

Peraltro è la stessa legge n. 24/2017 (c.d. legge "Gelli-Bianco") , nel suo primo articolo, secondo comma ad affermare espressamente che: *"La sicurezza delle cure si realizza anche mediante l'insieme di tutte le attività finalizzate alla prevenzione e gestione del rischio connesso all'erogazione di prestazioni sanitarie, e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative"*. [272] Dunque secondo la vigente normativa parrebbe proprio la struttura sanitaria ad essere responsabile del danno biologico eventualmente causato dal malfunzionamento, o blocco, tanto dei sistemi informatici, quanto dei dispositivi connessi (si pensi ad un *telerobot* adoperato in chirurgia), nel caso in cui non abbia adottato tutte le adeguate misure tecnico-organizzative atte alla prevenzione, nonché alla gestione del rischio.

4.12 Sicurezza dei dispositivi medici: scenari regolatori

Secondo l'Agenzia dell'Unione europea per la cybersicurezza [273] quando i dispositivi IoT supportano quelle che sono le funzioni principali di un ospedale, nozioni quali la sicurezza delle reti e dei sistemi informativi, unitamente alla protezione della privacy e dei dati relativi ai pazienti, diventano questioni critiche per quelli che sono definiti *smart hospitals*.

Si è infatti già ampiamente chiarito come la progressiva adozione di *connected medical devices* abbia condotto le strutture sanitarie ad una sempre maggiore vulnerabilità ed esposizione a incidenti ed attacchi informatici, potendo richiamare, a tal proposito, la nozione di *"Medical Devices Hijacking" (o Medjack)* per definire per l'appunto quegli attacchi che vedono come propri obiettivi i dispositivi medici (si pensi alle sopradette pompe d'infusione, o ai *pacemakers*). [274]

---

272 Legge 8 Marzo 2017, n. 24, recante *"Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie",* al sito https://www.gazzettaufficiale.it/eli/id/2017/03/17/17G00041/sg.

273 Il cui acronimo ufficiale è ENISA, dalla denominazione inglese *European Network and Information Security Agency.*

274 S. Meggitt, "Medjack attacks: the scariest part of the Hospital", in *Tufts University Press,* December 12th 2018.

Visti dunque gli impatti e le potenziali criticità correlati alla sicurezza dei dispositivi medicali, si vogliano ora prendere, celermente, in considerazione le regolamentazioni in materia, focalizzandosi sul panorama europeo. [275]

Innanzitutto si richiami il, già sopra ricordato, Regolamento Ue 2017/745 (MDR, dall'acronimo *Medical Device Regulation*), il quale ha profondamento rivisto la disciplina circa la produzione e la commercializzazione dei dispositivi medicali, così da aumentarne il livello di sicurezza (si pensi alla introduzione di una serie di studi clinici sia nella fase che precede l'ingresso del prodotto sul mercato, che in quella di sorveglianza post-vendita), nonché di rivedere ruoli e responsabilità dei soggetti coinvolti nell'articolato sistema di produzione e distribuzione. [276]

Uno dei pilastri, del suddetto Regolamento Ue, risulta essere la creazione di una banca dati europea sui dispositivi medici (EUDAMED, ossia *European Databank for Medical Devices*), operante come sistema collaborativo, di registrazione, catalogazione, notifica, nonché divulgazione di informazioni sui dispostivi, al fine di migliorarne trasparenza e condivisione, permettendo a tutti i soggetti interessati di accedere ad informazioni di base sui dispositivi medico-diagnostici (quali possono essere l'identità del dispositivo, il suo certificato, come anche gli operatori economici interessati agli aspetti di prestazione e sicurezza, etc.). [277]

Il MDR, nel suo secondo articolo, fornisce inoltre una lunga rassegna di definizioni, fra cui anche quella di fabbricante, indicato come *"la persona fisica o giuridica che fabbrica o rimette a nuovo un dispositivo oppure lo fa progettare, fabbricare*

---

275 La regolamentazione europea in tema di cybersicurezza dei dispositivi medicali, è arrivata indubbiamente in ritardo rispetto al contesto globale, prima del Gennaio 2020 infatti solo una netta minoranza di Agenzie degli Stati Membri aveva elaborato linee guida in materia: fra cui l'autorità francese ANSM *(Agence nationale de sécurité du médicament ed des produits de santé)* con l'emanazione nel 2019 di linee guida in materia di medical devices cybersecurity, o come anche l'Autorità tedesca BSI *(Bundesamt für Sicherheit in der Informationstechnik)* con la pubblicazione di raccomandazioni sotto forma di "requisiti di cybersicurezza per i dispositivi connessi".

276 La data di piena applicazione del Regolamento 2017/745, inizialmente prevista per il 26 Maggio 2020, è stata successivamente prorogata a causa dell'emergenza pandemica da Covid-19 al 26 Maggio 2021, data a partire dalla quale le sue norme sono divenute ed efficaci ed obbligatorie per tutti gli Stati Membri.

277 M. Franzo, F. D'Agostino et al., "Does a medical device nomenclature suitable for all purposes exist? Twenty years of Italian experience with the CND and its adoption in EUDAMED at European level", in the European Medical Device Nomenclature implementation working group project, Trieste, June 10th-12th, 2020.

o rimettere a nuovo e lo commercializza apponendovi il suo nome o marchio commerciale".

Tale soggetto dovrà garantire che i dispositivi da lui immessi in commercio siano conformi ai requisiti generali di sicurezza e prestazione definiti dal Regolamento Ue, effettuando a tale scopo la cosiddetta "valutazione clinica", prevista dall'articolo 61, circa l'idoneità del dispositivo ed i suoi eventuali effetti collaterali. Una volta conclusa poi la previa fase di valutazione della conformità del dispositivo, il fabbricante dovrà andare a redigere la documentazione tecnica, apporre il marchio CE, assegnare un codice UDI al prodotto medicale,[278] iscriverlo nella banca dati *Eudamed* e realizzare l'etichettatura.

Per quel che riguarda poi gli obblighi post-commercializzazione egli stesso dovrà, al fine di garantire la massima tracciabilità del dispositivo, realizzare un adeguato piano di sorveglianza ed adottare tutte le procedure interne atte alla segnalazione all'autorità competente di qualsiasi incidente grave e/o azione correttiva di sicurezza.

Si puntualizzi come, qualora il fabbricante di un dispositivo medico abbia sede in un territorio extra UE, l'immissione in commercio avverrà ad opera dell'importatore, definito per l'appunto come *"qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato dell'Ue un dispositivo originario di un paese terzo"*. Sull'importatore (come anche sulla figura del distributore)[279] grava parimenti l'obbligo di controllare la conformità del dispositivo al Regolamento MDR, come anche un generale obbligo di cooperazione con le autorità competenti al fine di attenuare i rischi eventualmente presentati dai dispositivi medicali commercializzati.

Ancora, il regolamento rafforza la figura del mandatario, ossia *"qualsiasi persona fisica o giuridica stabilita nell'Unione, che ha ricevuto ed accettato dal fabbri-*

---

278 L'identificazione unica dei dispositivi (UDI) è un codice numero o alfanumerico unico, associato ad un determinato dispositivo medico, che permette di indentificare in modo chiaro ed inequivoco i dispositivi immessi sul mercato, facilitandone di conseguenza la tracciabilità.

279 Definito dal Regolamento all'art. 2, par. 34) come *"qualsiasi persona fisica o giuridica nella catena di fornitura diversa dal fabbricante o dall'importatore, che mette a disposizione sul mercato un dispositivo, fino al momento della messa in servizio"*

cante avente sede fuori dall'Unione, un mandato scritto che la autorizza ad agire per conto del fabbricante in relazione a determinate attività con riferimento agli obblighi del medesimo", quest'ultimo sarà tenuto al controllo formale della documentazione comprovante la conformità del dispositivo medico, alla registrazione in Eudamed, ed infine sarà responsabile in solido col fabbricante per eventuali *medical devices* difettosi immessi in commercio.

Si noti oltretutto come venga prevista, ex art. 15, la nuova figura della *"Persona responsabile del rispetto della normativa"*, la quale possieda le competenze necessarie nel settore dei dispostivi medici, che sia nominata dai fabbricanti (e dai mandatari), col compito di assicurarsi che la conformità dei dispositivi sia adeguatamente controllata, che la documentazione tecnica sia redatta correttamente ed aggiornata, nonché che siano soddisfatti tutti gli obblighi in materia di sorveglianza post-commercializzazione.

Ovvio è che il MDR dovrà coordinarsi con altre normative europee, prima fra tutte il Regolamento Ue 2016/679 (GDPR). I moderni dispositivi medici sono infatti in grado di trattare importanti quantità di dati personali relativi alla salute, sicché la corretta gestione dei suddetti dati diviene un requisito necessario di sicurezza del dispositivo: ogni attore, coinvolto nel sistema, dovrà determinare proprie policy per raggiungere la compliance al GDPR, tenendo in dovuto conto i diritti degli interessati, la necessità di utilizzare i dati solo per i fini per cui siano stati raccolti, come anche l'adozione e l'implementazione di adeguate misure tecnico-organizzative atte alla protezione dei dati sensibili ed alla rilevazione di eventuali violazioni.

È invero nell'allegato I del MDR che risiedono elencati i *"requisiti di sicurezza e prestazione",* che devono esser rispettati da parte di ogni dispositivo medicale, affinché i rischi noti e prevedibili vengano ridotti al minimo, risultando anzi accettabili rispetto ai benefici, valutati per il paziente e/o l'utilizzatore del dispositivo stesso.

Specificatamente, si prevede come i fabbricanti debbano implementare, stabilire, documentare e mantenere un sistema di gestione del rischio, quale *"processo iterativo continuo"* durante l'intero ciclo di vita di un dispositivo, necessitante di un costante e sistematico aggiornamento.

Nel suddetto piano di gestione del rischio i fabbricanti dovranno infatti:

a. Individuare ed analizzare i pericoli noti e prevedibili associati a ciascun dispositivo;

b. Stimare e valutare i rischi associati, che si verifichino sia durante l'uso previsto, che durante l'uso scorretto ragionevolmente prevedibile;

c. Valutare l'impatto delle informazioni (relative ai pericoli ed alla loro frequenza, alle stime dei relativi rischi, nonché al complessivo rapporto benefici-rischi e all'accettabilità del rischio stesso) provenienti dalla fase di produzione e, in particolare, dal sistema di sorveglianza post-vendita;

d. In base alla previamente detta valutazione d'impatto, eventualmente, qualora sia necessario, modificare le misure di controllo del rischio che siano state adottate.

Chiaro è come per una corretta riduzione del rischio (si pensi a ciò che concerne gli errori d'uso) i fabbricanti dovranno anche considerare il livello di conoscenza tecnica, esperienza, istruzione, formazione, ed ambiente d'uso, come anche, laddove possibile, le condizioni mediche e fisiche degli utilizzatori previsti.

Non si dimentichi peraltro come rientrino nell'accezione di dispositivo medico anche i software (si pensi ad un *database* contente le cartelle cliniche dei pazienti), che il fabbricante sarà tenuto parimenti a realizzare in modo da eliminare o mitigare per quanto possibile i rischi correlati, compresi quelli associati ad una possibile interazione negativa tra il software stesso e l'ambiente IT in cui opera. Oltretutto sarà opportuno accertare che gli operatori sanitari che utilizzano il software rispettino le indicazioni del fabbricante, ad esempio in merito alle compatibilità tra software e hardware, alle caratteristiche delle reti IT e alle misure di sicurezza (quali quelle di protezione contro accessi non autorizzati).

Rimanendo sul tema, recentemente l'organismo europeo *Medical Device Coor-*

dination Group (MDCG) [280] ha pubblicato una Guida (dal titolo *"Guidance on Cybersecurity for medical devices"*) dedicata proprio agli standard ed ai requisiti di sicurezza, indirizzata ai fabbricanti di dispositivi medici, ponendo particolare attenzione alle nozioni di vulnerabilità e di *cybersecurity*. [281]

Non si tratta certo di uno strumento vincolante, ma ad ogni modo atto ad offrire un dettagliato quadro circa i requisiti in tema di sicurezza informatica, tali da garantire che l'utilizzo dei *medical devices* non vada a minacciare o compromettere le condizioni cliniche dei pazienti, né la sicurezza degli utilizzatori, oltre quella che viene individuata come normale soglia di rischio ritenuta "accettabile" (operando tramite la cosiddetta *"Benefit-Risk Analysis"*).

Si capirà infatti come raggiungere un equilibrio rischi-benefici nell'uso di un medical device sia quantomai delicato: se misure deboli potrebbero rivelarsi insufficienti a prevenire una violazione (come qualsiasi *cyber-threat*), anche misure troppo restrittive potrebbero altresì impedire il buon funzionamento di un dispositivo (si pensi ai casi di emergenza medico-sanitaria, in cui il personale addetto dovrà poter avere rapido accesso ad un dispositivo cardiaco, senza alcuna restrizione).

Nelle linee guida vengono inoltre ribaditi e rafforzati gli obblighi in capo ai produttori sia pre-mercato (identificando requisiti minimi di sicurezza *by design,* da adottare in fase di sviluppo, progettazione e fabbricazione dei *devices*), sia post-vendita, in quest'ultimo caso, al verificarsi di un incidente cyber, si evidenzia come i produttori siano tenuti a svolgere una apposita indagine, nonché ad effettuare una notifica alle autorità competenti in modo da informarle circa la natura del *cybersecurity breach* e dei possibili effetti negativi registrabili sulla salute degli interessati.

L'obiettivo di tale Guida risulta comunque quello di suggerire una oculata gestio-

---

280 Il Medical Device Coordination Group della Commissione Europea è stato istituito proprio con l'emanazione del Regolamento Ue 745/3027 MDR)

281 Medical Device Coordination Group (MDCG), *Guidance on Cybersecurity for medical devices,* December 2019, per una integrale consultazione si rimanda al sito istituzionale https://ec.europa.eu/docsroom/documents/41863.

ne del rischio, in cui quindi il modello da seguire sia il noto *risk-based approach* (già sancito con l'entrata in vigore del GDPR), da coniugarsi necessariamente con una valutazione *case by case*: affinché il rischio associato al funzionamento dei dispositivi medicali sia accettabile, si dovrà garantire un livello accettabile di protezione di salute e sicurezza (ossia, *safety e security*), proprio perché un adeguato livello di sicurezza informatica e resilienza dei dispostivi medici risulta essere proprio l'elemento cruciale per il mantenimento dell'erogazione quotidiana degli stessi servizi sanitari. [282]

282 Studio Legale DLA Piper, "Cybersecurity nell'uso dei dispositivi medici: nuova guida del Medical Device Coordination Group", in *Diritto al Digitale,* 21 Gennaio 2020.

CAPITOLO 5

PREVENIRE PER CURARE

5.1 Il panorama normativo della cybersecurity

Nella sua accezione più generale la *cybersecurity* viene presentata quale semplice estensione del concetto di "sicurezza informatica", [283] tuttavia certo è che limitare suddetto concetto alla sola protezione dei sistemi informativi risulta tanto fuorviante, quanto anacronistico. Di gran lunga più attuale si dimostra la definizione riportata all'interno dello standard ISO/IEC 27032:2012 (per come rivisto e confermato nel 2018), che rievocando le componenti della triade CIA, si appresta a designare la cybersicurezza come: *"la pratica che consente ad una entità di proteggere i propri asset fisici, come anche la confidenzialità, l'integrità e la disponibilità delle proprie informazioni, da quelle minacce che provengono dal cyberspace."* [284]

Il contesto in cui si suole operare è pertanto infinitamente più complesso di un semplice computer (o di una rete internet), consistente nel cyberspazio tutto, inteso quale *complex environment*, composto dalla costante interazione tra fattore umano, software e servizi. [285]

È innegabile difatti che il problema della *cybersecurity* coinvolga un vasto insieme di soggetti del moderno mondo digitale, si prenda da esempio il settore *dell'healtcare:* quando le organizzazioni sanitarie abbracciano la trasformazione digitale, diventano più aperte agli scambi con un ecosistema ampio composto da pazienti, partner, fornitori terzi, ed autorità sanitarie governative, il tutto in un ambiente di cura integrata e collaborativa. Dal momento che parallelamente allo sviluppo tecnologico, è proliferata anche la frequenza ed il grado di raffinatezza dei cyber attacchi, la sicurezza informatica risulta ad oggi la conditio sine qua non per la stessa innovazione: gli strumenti di sicurezza

---

283 Così la definizione fornita dal dizionario *Merriam-Webster: "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack",* per come disponibile al sito internet https://www.merriam-webster.com/dictionary/cybersecurity

284 ISO/IEC 27032: 2012, "Information technology – Security techniques – Guidelines for cybersecurity", July 2012, reperibile al sito internet https://www.iso.org/standard/44375.html

285 P. Montessoro, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Istituzioni del federalismo,* n.3, 2019, pp. 783-800.

devono saper gestire e "stare al passo" con la progressiva e repentina digitalizzazione. [286]

La *cybersecurity* pertanto altro non è che un'attività di prevenzione, basata sul principio fondante, diffuso tra gli esperti di sicurezza, che recita *"paranoia is a virtue":* non ci si può d'altronde affidare alla speranza che un evento avverso non accada, in quanto gli attuali automatismi dei sistemi di attacco rendono ogni dispositivo, sistema o servizio un possibile bersaglio. [287]

Diverse misure di tutela sono già state poste in essere per la protezione delle infrastrutture critiche [288] e dei servizi digitali nei Paesi dell'Unione europea, si vogliano pertanto passare in rassegna le principali normative susseguitesi nel tempo in materia di sicurezza informatica.

Posizione di spicco viene ricoperta dalla Direttiva (Ue) 2016/1148 recante *"misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi"* (c.d. Direttiva NIS, acronimo di Network and *Information security*), [289] recepita nel nostro ordinamento con il Decreto legislativo n. 65/2018, pubblicato sulla Gazzetta Ufficiale il 9 Giugno 2018 ed in vigore dal 24 Giugno dello stesso anno. [290] Così facendo l'Unione Europea ha voluto affrontare, con un approccio organico e trasversale, la sempre più emergente questione della *cybersecurity*, col fine di promuovere la cultura in materia di sicurezza cibernetica, rafforzare la resilienza delle infrastrutture nazionali ed altresì migliorare la cooperazione tra Stati membri.

---

286 Alcatel Lucent Enterprise, *Sicurezza informatica della rete sanitaria nell'era della trasformazione digitale: con una intervista speciale a Silvia Piai, Research Director per IDC Health Insights,* ALE international, 2020.

287 D.A. Wheeler, *Secure Programming HOWTO*, v3.72 Edition, 2015, p.16.

288 Per infrastrutture critiche (IC) si intendono i sistemi, i servizi, le reti o le risorse che, se danneggiati o distrutti, causerebbero gravi ripercussioni alle funzioni cruciali della società, tra cui la catena di approvvigionamenti, la salute, la sicurezza ed il benessere economico-sociale della popolazione.

289 Direttiva (UE) 2016/1148 (Direttiva NIS) del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, reperibile integralmente al sito internet https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148

290 Decreto Legislativo 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, reperibile integralmente al sito internet https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg

Come riportato nelle considerazioni introduttive della sopradetta Direttiva, le reti, i sistemi ed i servizi informativi svolgono un ruolo cruciale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone, e una loro perturbazione potrebbe sì avere ripercussioni non solo sui singoli Stati, ma in tutta l'Unione, danneggiandone l'economia nel suo complesso: si legge per l'appunto come la sicurezza delle reti e dei sistemi informatici siano essenziali *"per l'armonioso funzionamento del mercato interno"*. [291]

Si rilevi come il legislatore europeo, nel redigere il testo della Direttiva, non abbia adottato un orientamento prescrittivo (seguendo un approccio similare a quanto fatto con il GDPR), non disponendo cioè misure obbligatorie minimali da seguire pedissequamente, ma indicando semplicemente degli obiettivi generici da raggiungere, lasciando poi ai singoli soggetti un ampio margine di manovra nell'individuare ed implementare mezzi e strumenti considerati più idonei per il loro stesso raggiungimento. Si richiederà infatti genericamente che le misure di sicurezza adottate, sia a livello tecnico che organizzativo, siano proporzionate al rischio individuato, oltre che adeguate a prevenire e ridurre l'impatto che ogni incidente informatico potrebbe avere sulle reti e sui sistemi in uso, garantendo così la continuità del servizio offerto.

Come si evince poi dal testo del d.lgs. 65/2018, che ricalca accuratamente la Direttiva NIS, il settore sanitario, alla luce del suo impatto tanto economico quanto sul benessere e sulla qualità di vita della popolazione, è considerato una filiera strategica, rientrante pienamente nell'ambito della disciplina europea NIS, in particolare nella categoria dei c.d. *"Operatori di servizi essenziali"* (OSE).

Si chiarisce infatti come ogni Stato membro debba operare una attenta individuazione nel proprio territorio degli OSE, guardando a tutti quei soggetti, che siano pubblici o privati, operanti negli specifici settori elencati dall'allegato II della Direttiva (quali energia, trasporti, sanità, mercati finanziari, distribuzione di acqua potabile etc.), purché ex art. 5 :

---

291 R. Setola, G. Assenza, "Recepimento della direttiva NIS sulla cyber-security delle reti", in *Sicurezza e Giustizia*, n. IV, 2018, pp. 32-35.

a. Forniscano servizi essenziali per il mantenimento di attività sociali o economiche fondamentali;

b. La fornitura del servizio dipenda dalla rete e dai sistemi informativi;

c. Un possibile incidente abbia effetti negativi rilevanti sulla fornitura del servizio. [292]

Chiaro è come fra i soggetti suscettibili di essere nominati OSE nell'ambito sanitario verranno ricompresi tutti gli istituti sanitari (ospedali e cliniche private inclusi), e che l'autorità competente incaricata di tale individuazione sarà, ex art. 7 del Decreto attuativo, specificatamente il Ministero della salute, d'intesa con le Regioni e le Province autonome di Trento e Bolzano. Una volta identificati, gli Operatori di servizi essenziali saranno tenuti, ex art 12, ad adottare, *"tenendo in considerazione le conoscenze più aggiornate in materia"*, ogni misura tecnico-organizzativa atta a prevenire, gestire e minimizzare l'impatto di incidenti malevoli indirizzati a carico della sicurezza della rete e dei sistemi informatici utilizzati, al fine di assicurare la *continuity* dei servizi erogati.

Si ripeta come i testi normativi de quo non forniscano un elenco tassativo di misure da adottare, limitandosi invece ad esprimere un generico obbligo di implementare un livello di protezione e sicurezza adeguato al rischio esistente, che i soggetti saranno quindi chiamati a raggiungere in una autonomia relativa, tenendo cioè in debita considerazione tutte le linee guida e le *best practices* predisposte in materia dalle autorità competenti. [293]

---

292 Ex art 6 della direttiva NIS, per determinare la rilevanza degli effetti negativi si dovrà tener contro dei seguenti fattori: il numero di utenti e altri settori che dipendono dal servizio offerto dal soggetto interessato; l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza; la diffusione geografica relativamente all'aerea che potrebbe essere toccata da un incidente; l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura del detto servizio.

293 Quali le *Linee guida per gli operatori di servizi essenziali* (OSE), lavoro coordinato dalla Presidenza del Consiglio dei Ministri, dal Dipartimento delle informazioni per la sicurezza (DIS), in cooperazione con le autorità NIS di tutti i Ministeri, emanate in data 16 Luglio 2019.

Ulteriore obbligo gravante su tutti gli OSE (operatori nella filiera sanitaria inclusi) è poi quello di notificare, senza ingiustificato ritardo, al CSIRT italiano, ed alle autorità competenti NIS (ossia, i singoli Ministeri), eventuali incidenti in ambito cyber aventi un impatto rilevante sulla continuità dei servizi forniti, allegando le informazioni necessarie per constatarne portata e ripercussioni.

Il CSIRT (acronimo di *Computer Security Incident Response Team*), nasce invero dall'idea di fondere in un unico istituto [294] tutte le procedure di notifica, risposta e *recovery*, andando a migliorare così la cooperazione degli OSE e creando una maggiore consapevolezza in ambito di *cybersecurity*. Suddetta struttura poi, insieme ad altri organi di raccordo, avrà il compito di supportare la vittima di un cyber attacco fornendo tutte le informazioni e *l'expertise* necessari per facilitare una gestione efficace dell'evento dannoso, ed altresì per andarne a minimizzare le dirette ripercussioni.

Si aggiunga da ultimo come le autorità competenti NIS (trattando di sanità, il Ministero della salute e le Regioni), siano anche responsabili per l'attuazione della Direttiva NIS, vegliando sulla sua corretta applicazione, potendo invero richiedere agli OSE informazioni, documenti e dimostrazioni di aver adottato ed implementato tutte le misure di sicurezza adeguate. Difatti ex art 21 del Decreto n. 65/2018, le stesse autorità NIS possono applicare sanzioni pecuniarie amministrative laddove rilevino inosservanze da parte degli OSE circa il rispetto dei propri obblighi di sicurezza (si pensi alla non adozione di misure adeguate e proporzionate alla gestione del rischio, come anche alla mancata notifica al CSIRT italiano), comprese queste ultime fra i 12.000 ed i 150.000 euro per le violazioni più gravi.

A distanza di oltre sei anni dalla sua pubblicazione, pur risultando evidente il valore che la Direttiva NIS ha avuto nell'innalzare il livello di sensibilità degli Stati in materia di cybersicurezza, non si possono comunque sottacere anche i molteplici limiti che tale normativa ha palesato nella sua fase attuativa: non solo a causa dei recenti eventi pandemici che hanno certo mutato repentinamente il sistema

---

294 Proviene infatti dall'unificazione dei due *Computer Emergency Teams* preesistenti: il CERT nazionale ed il CERT-PA, quest'ultimo era pensato appositamente per i soggetti della pubblica amministrazione, dunque era precedente punto di riferimento degli ospedali pubblici.

socioeconomico globale o per la massiccia e costante digitalizzazione, ma anche per l'incapacità del legislatore europeo di prevedere la complessità di armonizzare quanto delineato nel testo normativo originario.

Tant'è vero che in un dettagliato report del 2019 la Commissione europea ha operato il punto della situazione proprio in tema di coerenza degli approcci assunti dagli Stati membri nella fase di adozione della Direttiva NIS. Così invero si legge: *"Sebbene la Direttiva NIS abbia avviato un processo fondamentale per aumentare e migliorare le pratiche di gestione dei rischi degli operatori in settori critici, vi è un notevole grado di frammentazione in tutta l'Unione"*. [295]

È proprio a causa del sopraricordato ampio margine di autonomia lasciato ai Paesi membri in fase di recepimento della Direttiva NIS che si sono venute a delineare fin da subito evidenti incertezze e disomogeneità su quali siano le misure di sicurezza da adottare ed implementare, su come identificare gli OSE, come anche sullo scambio di informazioni relative agli incidenti cyber a livello europeo.

Alla luce di tale scenario, e data l'urgenza di rafforzare le disposizioni della previa direttiva, la Commissione Europea ha avanzato, nel Dicembre 2020, una proposta di revisione, andando così a tracciare il percorso per la nascita di una direttiva nuova, che andrà ad abrogare e sostituire il testo precedente. [296]

È così che nel Dicembre 2022 la Direttiva Ue 2022/2555 (anche chiamata NIS 2) è stata pubblicata in Gazzetta Ufficiale dell'Unione europea, per entrare in vigore in data 17 Gennaio 2023, momento dal quale gli Stati membri avranno a disposizione ventuno mesi per adottare e pubblicare i relativi atti nazionali di recepimento. [297]

---

295 Commissione Europea, *Relazione della Commissione al Parlamento Europeo e al Consiglio di valutazione della coerenza degli approcci adottati dagli Stati membri per l'identificazione degli operatori di servizi essenziali conformemente all'articolo 23, paragrafo 1, della direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi,* Bruxelles 28.10.2019, per reperire il report integralmente si guardi al sito https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52019DC0546&from=EN

296 Commissione Europea, *Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148,* Bruxelles 16.12.2020

297 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), in Gazzetta Ufficiale dell'Unione Europea, L333, 27 Dicembre 2022.

Ovvio è che la suddetta Direttiva NIS 2 presenti svariati punti in comune con la preesistente normativa, al contempo però vede anche importanti novità, fra cui un maggiore ambito di applicazione: il legislatore europeo ha infatti arricchito il ventaglio degli attori, includendo ulteriori soggetti a cui applicare le disposizioni normative, appartenenti a settori definiti "ad alta criticità", fra cui si ricordino in questa trattazione i produttori farmaceutici, come anche i fabbricanti di dispositivi medici e medico-diagnostici in vitro.

Tali soggettivi attivi peraltro non verranno più identificati dai singoli Stati membri liberamente, ma anzi si seguiranno criteri condivisi ed uniformi così da permettere una più coerente ed organica identificazione degli operatori, pubblici e privati, da assoggettare alla nuova disciplina, evitando l'applicazione di criteri disomogenei fra Paesi membri. [298]

Nonostante resti fermo poi, ex art 21, l'obbligo di adottare misure tecniche, operative ed organizzative adeguate e proporzionate alla gestione dei rischi, viene al contempo aggiunta un'elencazione di misure specifiche, che dovranno essere necessariamente adottate, andando così a limitare la precedente piena discrezionalità dei Paesi membri, fra le cui misure si rinvengono:

a. a) politiche sull'analisi dei rischi e sulla sicurezza dei sistemi informatici;

b. b) sistemi di gestione degli incidenti;

c. c) strategie di *business continuity* (come la gestione dei backup o anche il *disaster recovery*); [299]

d. d) misure di gestione circa la sicurezza della *supply chain* (c.d.

---

298 Si evidenzi peraltro come la Direttiva NIS 2 suddivida i propri attori in *"soggetti essenziali"* (settore di energia, trasporti, sanità, pubblica amministrazione, infrastrutture digitali etc.) e *"soggetti importanti"* (produzione e distribuzione di prodotti chimici, fornitori digitali, servizi postali, produzione di apparecchiature medicali etc.): ai primi si applicherà un rigoroso regime di vigilanza ex ante, mentre i secondi saranno sottoposti ad una vigilanza ex post che interverrà in caso di rilievi o segnalazioni di non conformità.

299 Per *Disaster recovery* si intende quell'insieme di azioni e strategie operative, logistiche ed organizzative che una azienda mette in atto per mettere al sicuro e ripristinare i propri dati e la propria infrastruttura IT in seguito ad una interruzione forzata causata da un evento straordinario, sia esso di tipo accidentale, colposo o volontario.

catena di approvvigionamento), compresi tutti gli aspetti in materia di sicurezza riguardanti i rapporti tra ciascun soggetto ed i suoi diretti fornitori;

e. e) sicurezza circa l'acquisizione, lo sviluppo e la manutenzione dei sistemi informatici, comprese la gestione e la divulgazione delle vulnerabilità;

f. f) pratiche di igiene informatica base e formazione in materia di sicurezza informatica;

g. g) politiche e procedure relative all'uso della crittografia e della cifratura;

h. h) misure in materia di sicurezza delle risorse umane, politiche di controllo degli accessi e di gestione degli asset;

i. i) l'utilizzo di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza.

Fisso resta inoltre l'obbligo di notificazione alle autorità competenti circa gli incidenti cyber che abbiano un impatto significativo sulla continuità e fornitura del servizio, ed anche circa qualsiasi minaccia informatica che potrebbe aver potenzialmente provocato un incidente significativo (c.d. *near miss*), tuttavia nella NIS 2 viene regolamentato l'iter in maniera più dettagliata, prevedendo la trasmissione di un *"early warning"* (ossia di un preallarme) entro il termine di 24 ore dalla conoscenza dell'incidente, seguito, entro 72 ore, dalla notifica di una sua analisi dettagliata, che aggiorni oltretutto le informazioni fornite col primo preallarme. [300]

Si osservi ancora come la nuova Direttiva *de quo* preveda poteri minimi di indagine in capo alle autorità nazionali affinché valutino l'adeguatezza delle misure concretamente adottate, con la rinnovata possibilità di applicare sanzioni ammi-

300 D. Pierattoni, "La direttiva NIS2: nuovi obblighi e opportunità", in *Sicurezza e Giustizia*, V. II, MMXXII, pp.34-37

nistrative pecuniarie in caso di rilevate violazioni (si pensi ad una mancata notifica), per un massimo di almeno 10 milioni di euro, o fino al 2% del fatturato globale annuo dell'anno precedente dell'impresa (si noterà come rispetto alla previa disciplina NIS si sia avuto un incremento sanzionatorio importante).[301]

Le sopra analizzate direttive rimangono comunque solamente uno dei tasselli del complesso universo normativo della *cybersecurity* nell'ambito *healthcare*, dovranno infatti essere affiancate a tutti gli altri strumenti legislativi europei, rilevanti per gli operatori del settore sanitario, di cui peraltro già si è discusso in precedenza: si ricordi il Regolamento Ue 2016/679 (ossia il GDPR) riguardante il trattamento dei dati personali, ed i Regolamenti 2017/745 (MDR, *European Medical Devices Regulation*) e 2017/746 (IVDR, *In-vitro Diagnostics Regulation*). Di recente poi si è raggiunto un accordo circa l'approvazione della Direttiva sulla resilienza delle infrastrutture critiche (Critical Entities Resilience, CER), per come proposta dalla Commissione Europea nel Dicembre 2020.[302]

La CER andrà sostituire la Direttiva 2008/114/CE (ECI),[303] che peraltro si applicava solo ai settori dell'energia e dei trasporti, occupandosi nello specifico della sicurezza cyber relativa alle entità "altamente critiche" (fra cui, il settore della sanità) e della loro resilienza rispetto a una serie di possibili minacce, sia naturali che antropiche. Ai sensi della Direttiva de quo ogni Paese membro sarà chiamato ad adottare una strategia nazionale *risk based,* assicurandosi che tutti i soggetti critici adottino ogni misura tecnico-organizzativa atta a prevenire gli incidenti, proteggere fisicamente le aree sensibili, mitigare le conseguenze malevoli, gestire la sicurezza dei dipendenti ed aumentare il livello di *awareness* fra il personale.

SI capirà allora come la Direttiva CER si vada ad inserire in un panorama già com-

---

301 Si specifichi che se un incidente informatico ha comportato anche un *data breach* per come disciplinato dal GDPR, da cui è derivata una sanzione ai sensi del Regolamento privacy europeo, le sanzioni amministrative della Direttiva de quo non saranno applicabili.

302 European Commission, *Proposal for a directive of the european parliament and of the council on the resilience of critical entities,* Bruxelles 16.12.2020, reperibile integralmente al sito internet https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829

303 Direttiva 2008/114/CE del Consiglio, dell' 8 dicembre 2008 , relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (Testo rilevante ai fini del SEE), in *Gazzetta Ufficiale dell'Unione Europea,* L345/75, 23.12.2008.

plesso e ad oggi sempre più interconnesso, ponendo un approccio nei confronti delle infrastrutture "altamente critiche" più ampio ed inclusivo, così peraltro dichiara in Conferenza stampa Ylva Johansson, Commissario Europeo per gli Affari interni: *"Alla luce dell'attuale situazione geopolitica in Europa, rafforzare la nostra resilienza è di fondamentale importanza. La Direttiva CER ci renderà maggiormente preparati ad affrontare le perturbazioni che incidono sulla sicurezza dei nostri cittadini e sulla prosperità del mercato interno [...]. La nuova Direttiva garantirà infatti la fornitura di servizi essenziali come l'energia, i trasporti, l'acqua, l'assistenza sanitaria, riducendo al minimo l'impatto degli incidenti che siano naturali, o provocati dall'uomo."*[304]

5.2 Linee guida ENISA

In materia di *cybersecurity* è indubbio che si possa ivi rimarcare anche l'operato svolto da ENISA (acronimo di *European Network and Information Security Agency*), quale Agenzia dell'Unione europea mirante a conseguire un elevato livello condiviso di cybersicurezza in tutto il panorama comunitario. Sono ormai oltre quindici anni difatti che l'anzidetta Agenzia svolge un ruolo fondamentale nel rafforzare la sicurezza digitale in tutta Europa, contribuendo positivamente a consolidare le capacità di preparazione e di risposta degli Stati membri in caso di incidenti informatici.[305]

Guardando poi alle sue nuove pubblicazioni, per ciò che più sta a cuore alla presente trattazione, si riporti la recente relazione dal titolo: *"Procurement guidelines for cyber security in hospitals",* in cui l'Agenzia ha voluto raggruppare tutta una serie di prassi e raccomandazioni, applicabili a livello ospedaliero, atte a garantire la sicurezza dei propri sistemi.

---

304 *Press release* in occasione dell'accordo raggiunto fra Parlamento Europeo e Consiglio dell'Unione Europea circa l'approvazione della Direttiva CER, "Security Union: Commission welcomes today's political agreement on new rules to enhance the resilience of critical entities", 28 June 2022, Bruxelles.

305 ENISA, *Un Europa affidabile e sicura dal punto di vista informatico: Strategia Enisa,* Agenzia dell'Unione europea per la cibersicurezza, Atene, Giugno 2020.

Nelle note introduttive invero l'Agenzia asserisce come la *cybersecurity* sia diventata sempre più una assoluta priorità per le strutture ospedaliere, tale da dover essere ad oggi fortemente integrata in tutti i processi, fasi e componenti che vadano a caratterizzare ed influenzare l'ecosistema ICT sanitario. [306]

In particolare la guida fa riferimento all'ambito del *procurement* in sanità, inteso quale processo di approvvigionamento indirizzato all'ottenimento di beni, servizi o lavori da una fonte esterna che siano necessari per l'azienda, ottenuti spesso tramite procedura di gara od offerta competitiva. [307]

Pertanto il *procurement* va a rivestire indubbiamente un *key role* all'interno di una qualsivoglia struttura sanitaria, dato il suo compito strategico di gestirne efficacemente il *budget*, provvedendo all'ottenimento delle risorse necessarie al perseguimento degli obiettivi aziendali.

Al fine di chiarire quali siano i sistemi ed i dispositivi rientranti negli acquisti sanitari, ENISA avvia il report delineandone una tassonomia, comprendente:

a. sistemi informativi clinici (ossia software orientati all'assistenza medica, quali i *Laboratory Information System* [308] *o i Drug Databases*);

b. dispositivi medici (qualsiasi componente hardware che sia destinato al trattamento, controllo o diagnosi di malattie, quali: apparecchiature di radiologia, robot chirurgici, pompe per infusione, dispostivi impiantabili come *pacemakers*, *holters*, defibrillatori cardiaci, infusori per l'insulina etc.);

---

306 ENISA, *Procurement guidelines for cybersecurity in hospitals: good practices for the security of Healthcare services,* European Union Agency for Cybersecurity, Athens Office, February 2020, reperibile al sito internet https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

307 Si precisi come il termine appalto, nella sua connotazione giuridica, sia inteso come procedura, quale *corpus* di principi e regole, che il legislatore italiano ha previsto quando una istituzione soggetta alla regolazione giuridica pubblica acquista o vende sul mercato beni, servizi ed opere. Tuttavia si vanno ad oggi via via ampliando i tradizionali modi di intendere l'attività d'appalto permettendo di comprendere fattispecie contrattuali diverse dal contratto di appalto stesso, quali la somministrazione, la locazione finanziaria o la concessione. Cfr. E. Pintus, *Scelte pubbliche e strumenti di management per gli acquisti,* McGraw-Hill, Milano, 2009.

308 Per *Laboratory Information System* (LIS) si intende un particolare tipo di software utilizzato nei laboratori di analisi per la gestione integrata di molteplici tipi di dati e processi.

c. apparecchiature di rete (cavi, routers, *firewalls*, reti VPN etc.);

d. sistemi di assistenza remota;

e. sistemi di identificazione (per identificare pazienti o medici, garantendo che non vi siano accessi non autorizzati, fra cui gli scanner biometrici);

f. sistemi di gestione degli edifici (linee elettriche, tubature e qualsiasi tipologia di costruzione che possa ospitare strumentazioni mediche,);

g. servizi professionali (esternalizzati o meno, prestati da professionisti o società: servizi di trasporto, progettazione, contabilità, manutenzione consulenza legale etc.);

h. servizi cloud (quali sistemi informativi per la gestione dei rapporti con i clienti, che non siano ubicati nella struttura ospedaliera).

Com'è immaginabile ognuno di tali sistemi e dispositivi porta con sé fattori di rischio propri, esaminati da Enisa e legati ad errori nella progettazione, all'uso di protocolli non sicuri, a difetti di autenticazione che comportano accessi non autorizzati o talvolta anche ad una impropria implementazione degli stessi all'interno della struttura sanitaria.

Per fornire peraltro un quadro maggiormente completo circa le possibili minacce in cui ogni struttura ospedaliera può incorrere, l'Agenzia Ue raggruppa queste ultime in cinque macrocategorie, in base alla loro origine:

a. ***Natural phenomena:*** sebbene rappresentino i rischi più remoti, vi si possono ricomprendere tutti gli eventi naturali disastrosi come incendi, allagamenti, terremoti. Non è raro peraltro che diverse strumentazioni (quali per le risonanze magnetiche o le radioterapie) siano localizzate ai piani interrati, divenendo di conseguenza maggiormente esposte a tali fenomeni;

b. ***Malicious actions:*** si ripeta come nelle organizzazioni sanitarie i sistemi IT siano fortemente interconnessi e difficili da isolare senza ingenerare una interruzione del servizio erogato, creando un fertile ecosistema per i cybercriminali. ENISA altro non fa che elencare nel dettaglio le azioni malevoli che potrebbero toccare *l'health system,* su cui già la suddetta trattazione si è soffermata: malware (virus, *ransomware* etc.), attività di social engineering (si pensi al phishing), manomissione dei dispositivi medici (*Medjacking*), attacchi DoS, cyber spionaggio (celato dietro ad interessi di industrie farmaceutiche), furti d'identità e compravendita di dati sanitari;[309]

c. ***Supply chain failure:*** non tutti i servizi sono infatti localizzati nei server ospedalieri, ma possono essere esternalizzati e dipendere da servizi cloud o di rete relativi a fornitori terze parti (gli stessi dispositivi IoMT funzionano nel cloud). Pertanto se i *provider* non si adoperano per garantirne il funzionamento anche *off-line,* ciò potrebbe inevitabilmente causare gravi interruzioni nella erogazioni dei servizi sanitari. Rientrano in tale categoria anche tutti i possibili guasti, errori di *design*, e di progettazione relativi ai dispositivi medicali;

d. ***Human errors:*** vengono ivi ricomprese dalle minacce connesse ad una mancanza di compliance e *policies* efficaci, a *default* password deboli, sistemi mal gestiti, accessi non autorizzati, fino ad errori di inserimento dei dati sanitari da parte del personale medico;

e. ***System failures:*** i guasti del sistema possono essere relazionati ad avaria dei software, a mancati aggiornamenti dei *firmware*, ad una insufficiente manutenzione o alla non disponibilità dei sistemi per sovraccarichi di rete.

---

309 S. Smith and R. Koppel, "Healthcare Information Technology's Relativity Problems: A Typology of How Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ", in *Journal of the American Medical Informatics Association*, 21, no. 1, January 2014, pp. 117–31.

Si capirà la motivazione di tali premesse: è di fondamentale importanza conoscere, studiare e parametrare ogni possibile minaccia che possa intaccare una struttura ospedaliera al fine di poter dare priorità a tutti quei prodotti e/o servizi che si rivelano esposti e particolarmente sensibili.

Ed è così che l'agenzia ENISA arriva a disporre in elenco specifiche *good practices* da adottare cosicché qualsiasi operatore IT sanitario possa avere un ottimo punto di partenza nell'acquisire apparecchiature ospedaliere. [310]

Si segnali peraltro come suddetta serie di buone prassi e raccomandazioni sia il risultato raggiunto per il tramite di contributi ottenuti dai molteplici operatori sanitari intervistati. In suddette *good practices* si suole raccomandare di:

a. Coinvolgere il dipartimento IT ospedaliero nelle diverse fasi di scelta e valutazione circa la fornitura di beni e servizi, così da garantire che non vengano tralasciati gli aspetti relativi alla cybersicurezza;

b. Attuare ed implementare una procedura di identificazione e gestione delle vulnerabilità ancor prima di acquisire i nuovi sistemi, prodotti e/o servizi, e mantenerla per tutta la durata del loro ciclo di vita;

c. Tener in stretta considerazione gli aspetti riguardanti l'interoperabilità, al fine di garantire l'assenza di divari in termini di sicurezza rispetto alle componenti già esistenti nella struttura informatica preesistente;

d. Sviluppare una policy per gli aggiornamenti *hardware* e *software* che assicuri l'installazione delle patch più recenti (sia sui sistemi operativi che sugli *antivirus*, *firewall* etc.);

---

310 Peraltro il *Procurement* viene tripartito da ENISA in tre fasi: la *plan phase* (in cui l'ospedale analizza e studia i propri bisogni e necessità), la *source phase* (dove viene avviata la procedura di approvvigionamento, momento in cui l'ospedale riceve le relative offerte, valutando e selezionando i prodotti/servizi più adeguati, procedendo poi all'aggiudicazione del contratto), ed infine la *manage phase* (in cui si monitorano le effettive performance dei sistemi, servizi e/o dispositivi in modo tale da poter porre in essere eventuali misure correttive).

e. Programmare periodici test sulla sicurezza sia dei prodotti, fra cui i test anti-intrusione (c.d. *penetration* test), sia dei sistemi (l'accesso alle reti *wireless* ospedaliere dovrà essere rigorosamente limitato e controllato), così da poter eventualmente adottare misure correttive;

f. Progettare piani di azione a garanzia della *business continuity,* atti cioè ad assicurare che un guasto del sistema non causi l'interruzione in toto dei servizi essenziali erogati dall'ospedale;

g. Garantire la sicurezza dei *log* di accesso ai sistemi per prevenire ed intervenire sugli eventuali accessi non autorizzati all'interno dei sistemi, ed essere comunque in grado di tracciare l'entità delle informazioni perse o rubate una volta che il sistema sia stato compromesso;

h. Crittografare i dati personali sensibili che siano conservati o diffusi, per il tramite di una policy per sistemi, servizi e dispostivi ex art. 9 GDPR;[311]

i. Fornire una adeguata formazione sulle prassi di *cybersecurity* così da garantire che il personale interno ed anche i contraenti esterni siano correttamente preparati circa tutti i rischi connessi a prodotti o servizi recentemente acquisiti.

Volendo concludere, non basterà dotare la propria infrastruttura IT di una serie di *tools* e pensare di aver in tal modo conferito sicurezza all'intera struttura ospedaliera, viceversa occorrerà mettere in atto una strategia olistica di "difesa in profondità", attuata mediante una metodologia globale di gestione del ciclo di vita della *cybersecurity*, che parta cioè dall'analisi e dalla valutazione dei rischi, all'adozione di idonee architetture di sistema, per arrivare alla gestione e monitoraggio in tempo reale di sistemi e servizi sanitari. Il tutto attraverso soluzioni sì intrinsecamente sicure e resilienti che, pur offrendo sempre il livello massimo di

311 Medesime raccomandazioni sono state emanate dall'Istituto Superiore della Sanità il 17 Giugno 2019, nel Documento di indirizzo del Gruppo di Studio Nazionale sulla Cybersecurity nei servizi sanitari, dal titolo *"Buone pratiche per la sicurezza informatica nei servizi sanitari".*

sicurezza e di *business continuity* dei sistemi e servizi sanitari, non ne ostacolino mai al contempo la piena efficienza operativa.

5.3 Readiness, response, recovery

Si voglia ivi scendere ancora più nel dettaglio circa quali siano le concrete misure di sicurezza, metodi e strategie da dover adottare al fine di incrementare fortemente la protezione delle strutture critiche sanitarie. A tale scopo si analizzi la guida pratica *"Healthcare system cybersecurity"* elaborata nel 2022 da ASPR (*Administration for strategic preparedness and response*), Agenzia statunitense, operante all'interno del Dipartimento della salute e dei servizi umani, focalizzata ad operare nel settore della prevenzione, preparazione e risposta circa tutti gli incidenti che possano essere impattanti sulla salute pubblica. [312]

Il documento *de quo* si presenta suddiviso in tre sezioni, rappresentanti cronologicamente l'iter di sicurezza nel suo svolgersi, ossia per come costituito dalle fasi di: *Readiness, Response e Recovery*.

Si esordisca quindi guardando alla fase di preparazione (o mitigazione), quale momento in cui le strutture hanno l'incarico di fissare regolari *penetration tests,* scansioni delle *vulnerabilities*, nonché protocolli di monitoraggio, al fine di garantire una rapida identificazione delle possibili minacce. Man mano poi che tali vulnerabilità vengono rilevate, dovrebbero esser classificate in un ordine di priorità ed in seguito risolte per mezzo delle più recenti *patch* (quali modifiche, aggiornamenti, da qui letteralmente il "mettere una pezza") od altre attività propriamente di blocco. Ancora si dovranno porre in essere tecniche di *network segmentation* (si ripeta, comportano il partizionare una data rete ospedaliera in piccole sezioni, cosicché anche se un malintenzionato riuscisse ad infiltrarsi in una di queste, le altre rimarrebbero ad ogni modo sicure), ed altresì tecniche atte a gestire e con-

312 ASPR, *Healthcare system cybersecurity: Readiness & Response Considerations,* ASPR (Administration for strategic preparedness and response) – TRACIE (healthcare emergency preparedness information gateway), originally published February 2021, Updated October 2022.

trollare gli accessi (si pensi alle, già in precedenza trattate, autenticazioni multi-fattoriali od anche agli approcci *Zero Trust*).

Sempre in questa preliminare fase dovranno essere testati e regolarmente aggiornati i c.d. *Disaster recovery plans,* intesi quali piani di continuità operativa contenenti soluzioni dettagliate atte ad indicare come rispondere efficacemente a svariate tipologie di incidenti, al fine di ridurre al minimo ogni interruzione delle normali operazioni, limitare la portata dei danni, definire in anticipo specifiche modalità operative alternative, fornire un rispristino del servizio rapido, ed altresì addestrare il personale alle procedure di emergenza.[313]

In aggiunta dovranno essere assicurati anche i *Business contnuity plans* quali documenti ancora più completi dei precedenti, contenenti tipicamente una *checklist* comprendente i piani di emergenza per i processi aziendali, i beni, le risorse umane ed i partner commerciali, ossia circa ogni aspetto del business che potrebbe essere colpito. Assicurandosi sempre che suddetti *plans* vengano rispettati ed includano anche tutti i servizi ancillari ed *off-campus,* (si pensi alle sedi ambulatoriali od ai laboratori di analisi) e che prevedano l'eventualità che un'interruzione possa intaccare anche strutture sanitarie limitrofe, precludendo così il trasferimento dei pazienti critici.

Affinché poi gli anzidetti piani di *recovery* e *continuity* siano efficaci, sarà comunque necessario mantenere un robusto ed affidabile inventario circa tutti gli hardware, software, dati e dispostivi medici utilizzati, dei fattori che possano impattare sul loro funzionamento e come a loro volta questi stessi possano influenzare la salute del paziente, in particolare si dovranno identificare tutti i supporti critici vitali e salvavita (si pensi ai ventilatori polmonari od alle pompe infusionali) che potrebbero essere particolarmente vulnerabili a possibili attacchi informatici, assicurandosi di prevedere un loro efficace piano di backup.

Ovvio è poi che le strutture devono essere preparate a segnalare qualsiasi incidente insolito o comportamento anomalo del sistema (si pensi ad un riavvio

---

313 CINI-Cybersecurity National Lab, *Il futuro della Cybersecurity in Italia: ambiti progettuali strategici, progetti ed azioni per difendere al meglio il Paese dagli attacchi informatici,* Laboratorio Nazionale di Cybersecurity- CINI Consorzio interuniversitario Nazionale per l'Informatica, 9 Ottobre 2018.

non pianificato, un arresto, un *crash* od una interruzione di rete apparentemente casuale) non appena venga indentificato, tramite rapida segnalazione. Dunque altrettanto ovvio è che il personale tutto dovrà avere familiarità e formazione circa le modalità di *incident reporting*, ossia avendo ben chiaro a chi segnalare, quando farlo, ed altresì quali informazioni includere, creando a tal fine adeguati protocolli di notifica, o sistemi di comunicazione di massa, o anche applicazioni che consentano agli stessi dipendenti di ricevere *alerts* automatici durante una emergenza. Si potrebbe peraltro anche prendere in considerazione la possibilità di sviluppare un color code atto a comunicare agilmente i livelli idi sicurezza informatica, presupponendo che il personale comprenda il significato dei colori e le relative implicazione ed azioni da intraprendere.

Si riporti a tal fine la griglia elaborata dalla *Nebraska Medicine,* azienda sanitaria statunitense con sede a Omaha:

- ***Green:*** gli incidenti e le segnalazioni di sicurezza informatica sono ad un normale livello; gli strumenti e le protezioni funzionano correttamente.
- ***Yellow:*** gli incidenti e le segnalazioni di sicurezza informatica sono leggermente superiori al normale; gli strumenti e le protezioni non stanno funzionando correttamente.
- ***Red:*** gli incidenti e le segnalazioni di sicurezza informatica sono molto più elevati del normale; gli strumenti e le protezioni non funzionano e non risultano efficaci.

Ancora, prendendo atto di come il sistema sanitario si figuri quale una complessa catena multisoggettiva, occorrerà capire in che misura i fornitori terzi possano influenzare le prestazioni e la protezione dei sistemi critici, pianificare adeguati piani di risposta, basati sulla valutazione di come possano gli incidenti intaccare le risorse compromesse (si pensi ad una possibile interruzione della funzionalità di un sistema salvavita).

Data l'interoperabilità poi dei sistemi sanitari dotarsi di una c.d. *Application De-*

pendency Map (ADM) può aiutare a conferire una precisa mappatura di tutte le applicazioni e dispositivi, nonché delle interdipendenze reciproche, sicché, in caso di incidente informatico, venga seguito accuratamente un ordine di priorità nelle attività di ripristino, a seconda proprio del diverso grado di criticità di ogni tecnologia. Al fine di determinare suddetto ordine di priorità nella *restoration* occorre stilare invero un *ranking* circa il grado di impatto di un sistema, software o dispositivo compromesso nei confronti di:

a. Sicurezza del paziente e qualità della cura;

b. Numero di dipendenti e pazienti interessati dalla violazione;

c. Entrate perse;

d. Costi ed implicazioni legali;

e. Numero di pazienti dirottati presso altre strutture;

f. Danni reputazionali e legati all'immagine.

In combinazione con gli sforzi di mitigazione, sarà anche opportuno prepararsi opportunamente ai tempi di inattività (c.d. *downtimes*) dovuti ad un incidente cyber, ossia regolamentando il ciclo di vita dei documenti cartacei (disponendo istruzioni chiare su quali moduli usare ed in quale momento), ed altresì verificando che tutti i vari *supplies* (moduli, etichette, attrezzatura clinica manuale, chiavette USB etc.) siano prontamente disponibili all'occorrenza. Anche i tempi di inattività possono essere categorizzati in base al loro impatto sulla *continuity* aziendale (ad esempio di Categoria A se determinano 12 ore o meno di inattività, di Categoria B per un calo di oltre 24 ore, Categoria C per più di 3 giorni etc.), affinché in tal modo le attività di risposta siano parametrare sulla *severity* dell'incidente informatico.

Transitando ora alla successiva fase della *response*, ovvio è che quando si sospetta la verificazione di un incidente informatico, gli esperti IT inizieranno immediatamente a valutarne il livello di impatto sul sistema e sulle infrastrutture (sulla base dei criteri di gravità ed impatto previamente determinati). Mentre indagano

sulla entità del danno si muoveranno al fine di isolare, riparare o rimuovere le tecnologie interessate, cercando ad ogni modo di stabilizzare le prestazioni erogate e mantenere una assistenza sicura ai pazienti.

Una volta poi che minaccia e livello di impatto sono stati identificati, il team IT dovrà seguire i protocolli corrispondenti alla portata dell'evento informatico, dal momento che ogni tipologia di incidente differirà nel grado di impatto e richiederà una differente combinazione di risposte e strategie di *recovery*.[314]

È in tale momento che viene in gioco la capacità di essere resiliente di una struttura, gli stessi dipartimenti infatti dovranno poter richiedere e disporre di personale aggiuntivo (o riallocato) per far fronte ai periodi di interruzione ed inattività. Si dovrebbe dunque condurre in tempo reale un inventario di tutto il personale disponibile, così da poter pianificare un'eventuale redistribuzione ed allocazione delle risorse umane nei reparti maggiormente bisognosi di addetti supplementari (si pensi all'eventualità che degli infermieri da un'unità chirurgica vengano spostati per assistere alle attività di pronto soccorso).

È evidente che in tali redistribuzioni bisognerà garantire che la forza lavoro trasferita disponga delle competenze necessarie, che abbia familiarità con i flussi di lavoro operativi all'interno del nuovo dipartimento, sicché si garantisca sempre e comunque la sicurezza dei pazienti e l'erogazione di prestazioni efficaci. Certo è possibile che risulti necessaria una formazione *just-in-time*, in tal caso si prenda in considerazione la possibilità di affiancare il personale senior alle figure lavorative meno esperte. Da ultimo ancora si tenga aperta la possibilità di richiedere personale off-site, ossia proveniente da strutture terze non direttamente colpite dall'incidente informatico, al fine di integrare eventuali carenze operative.

A livello operativo poi se l'accesso all'EHR (*electronic heatlh record,* ossia la versione digitale della cartella clinica di un paziente) risulta limitato o non possibile, dovranno determinarsi le modalità con cui le varie informazioni sul paziente

---

314 Si può comunque optare per l'organizzazione di un *initial incident brief* comprensivo della leadership aziendale, dei capi di dipartimento, degli esperti tecnici, dei consulenti legali e del personale in materia di pubbliche relazioni, ove vengono identificate quali funzionalità da adottare siano disponibili, sicure e maggiormente efficaci

(anamnesi, farmaci, dati clinici etc.) debbano essere, anche se in forma cartacea, registrati e mantenuti. Si vadano a delineare poi le possibili opzioni atte a ridurre il volume dei pazienti (quali annullare gli appuntamenti non urgenti, dirottare le ambulanze verso strutture vicine etc.), stimando per quanto tempo debbano essere attuate in base alla durata prevista per l'evento, al fine di comunicare il tutto alle strutture sanitarie e partner circostanti. [315]

Si tenga inoltre a mente come durante un evento informatico, una efficace condivisione delle informazioni sia vitale per ottenere efficaci riposte e sforzi di ripristino e per salvaguardare le sicurezza dei pazienti. Si identifichi quindi il modo migliore per veicolare la messaggistica interna (si pensi alle piattaforme di collaborazione come Microsoft Teams o WebEx), al fine di agevolare le comunicazioni collaborative. Per quanto concerne invece la comunicazione con l'esterno, occorre essere preparati alle impellenti domande che si origineranno dai media (quale *"I nostri dati sono al sicuro?*"), cercando di comunicare, almeno nei primi periodi, esclusivamente con dichiarazioni scritte, tenendo monitorate costantemente le testate giornalistiche ed i social media per rimediare ad una possibile disinformazione o a lacune informative ed altresì per rimanere al corrente del sentimento pubblico generale.

Sempre nella fase di riposta avranno luogo infine le attività di *reporting* e monitoraggio, per le quali attività è necessario che il personale tutto conosca i protocolli di segnalazione e di notifica.

Si giunga quindi alla fase di *recovery*, che vede come assunto base il fatto che sarà proprio la gravità dell'attacco a determinare la durata del recupero.

Si sottolinei come i sistemi informativi di regola non vengano rispristinati immediatamente, anzi ogni modifica richiederà adeguati monitoraggi, nonché costanti aggiustamenti distribuiti lungo un elaborato processo di analisi.

Mano a mano che i sistemi ed i reparti vengono rispristinati, sarà infatti necessario valutarne il livello di vantaggio o dannosità generale, ad esempio se un siste-

---

315 Ministry of health Singapore, *Healthcare Cybersecurity Essentials*, CSA (Security Agency of Singapore), August 2021.

ma risulta solo parzialmente funzionante, ci si dovrà chiedere se le funzionalità mancanti possano ostacolare il flusso di lavoro od aumentare il rischio. Bisognerà inoltre pianificare la migrazione di tutta la documentazione manuale venutasi a creare nel periodo di inattività, facendola trasmigrare dal formato cartaceo a quello elettronico, una volta ottenuto il completo ripristino.

Ancora, non appena le condizioni lo consentano, dovranno essere riprese tutte le procedure diagnostiche e terapeutiche in precedenza sospese, attuando una procedura per contattare i pazienti i cui appuntamenti ambulatoriali sono stati di fatto posticipati, in modo tale da poterli riprogrammare. Se necessario, si pianifichi anche il rimpatrio di tutti i pazienti che sono stati trasferito in strutture sanitarie limitrofe. Ovvio è che il ripristino possa (e alle volte debba) comportare anche l'applicazione di patch ed aggiornamenti calati sui software e sulle apparecchiature mediche, cosicché venga ridotta una possibile reiterazione dell'incidente informatico.

In conclusione si definiscano i criteri per dichiarare concluso l'incidente ed il ritorno alle normali operazioni, avvisando le parti interessate e preparando dichiarazioni pubbliche finali per i media. Le azioni che sono state intraprese, i piani ed i correttivi attuati sono comunque informazioni utili da dover mantenere, così come i dati post-incident da conservare accuratamente in uno storage a ciò dedicato. Si completi da ultimo il processo di rifornimento, inventariando tutte le *supplies* necessarie.[316]

Avendo ad ora chiaro lo scenario normativo che attornia la cybersicurezza ospedaliera, come anche l'iter pratico di misure e strategie da adottare in caso di incidente informatico, rimane ivi da chiedersi cosa accada concretamente all'interno delle strutture sanitarie italiane, come venga percepito il rischio cyber, e quali siano gli ostacoli legati ad una corretta attuazione ed implementazione del massimo livello di sicurezza possibile.

A tale fine si vogliano riportare a seguire le riflessioni ed i pareri di due figure pro-

316 Per ulteriori approfondimenti si indichi CREST, *Cyber Security Incident Response Supplier Selection Guide,* Version 1, 2013; Osterman Research, *Cyber security in Healthcare,* Whitepaper, February 2020.

fessionali, tanto distinte quanto complementari, inserite a piena regola nell'organigramma sanitario, e di conseguenza nelle problematiche di sicurezza cyber che possano derivarne.

5.4 Intervista: nell'ottica di un clinico

Si voglia riportare a seguire la testimonianza diretta, uno spaccato reale e veritiero, per come derivante dalla prospettiva, nonché sensibilità, di un esperto clinico quale operatore sanitario che *day by day* si ritrova ad agire in un campo (si potrebbe dire *minato*) ed a dover tenere il passo rispetto ad una continua e rapida cyber-evoluzione che indubbiamente pone nuovi quesiti, problematicità e sfide ad una professione che oggi più che mai appare in forte sovraccarico.

Sin da subito invero le complessità si sono poste in evidenza con estrema lucidità, ovvio è che in ambito medicale si debba operare un netto discrimine fra chi si occupa del settore puramente clinico e chi si occupa di igiene informatica, organizzazione e management, tuttavia: *"È proprio da tale basilare distinzione che si nota il sorgere di una prima problematica: l'informazione ultrasensibile sanitaria, il dato digitale, l'utilizzo del macchinario o strumentazione medica è ad appannaggio esclusivo del clinico, e non dell'igienista, la qual cosa comporta necessariamente una esposizione a molteplici rischi, legata per di più ad una totale incoscienza ed inconsapevolezza rispetto a ciò che il clinico abitualmente mette in moto e pone in essere. Lo scenario quindi è semplice ed è il seguente: nessun clinico è realmente consapevole circa quanto egli stesso si espone e quanto a sua volta fa esporre un dato sensibile od un paziente"*.

Ebbene si prosegua domandando se possa capitare che gli stessi medici, nello svolgimento delle proprie abituali funzioni, si servano di mezzi non pensati e progettati specificatamente per l'ambito sanitario (si pensi all'uso improprio di una applicazione di messaggistica), bypassando così quel livello di sicurezza e protezione che dovrebbe viceversa esser pienamente garantito, la risposta in tal caso risulta immediata ed autentica: *"Abitualmente, o meglio quotidianamente,*

ricevo e-mail, contenenti dati relativi ai pazienti, da parte di altri clinici, che necessitano di ottenere un secondo parere. Questo, per quanto banale, risulta un chiaro indice di quella mancanza di consapevolezza di cui poc'anzi".

Pare ovvio, ma vale comunque la pena ribadire in questa sede che trovare un giusto equilibrio non sia affatto semplice: in ambito sanitario difatti l'adozione di una misura di sicurezza, se troppo debole, potrebbe apparire insufficiente a prevenire una qualsivoglia violazione (o *cyber-threat*), viceversa però, se troppo restrittiva, porterebbe comunque andar a nuocere e rallentare l'operato medico, si pensi ai casi urgenti relativi ad emergenze sanitarie.

Invero così si vuole proseguire: *"È comunque una strada che continua ad essere seguita, per esigenze che sono tanto comodità quanto di celerità, ossia per ricevere e fornire risposte rapide ed esaustive in tutti quei casi che siano necessitanti di un celere consulto medico."*

Rimane purtuttavia vero il fatto che esistano tutta una serie di sistemi atti ad agevolare la complessità della realtà sanitaria: dalla cartella elettronica a livello regionale, fino all'odierna implementazione del S.I.O (Sistema informativo Ospedaliero) che intende perseguire il progetto di affinare la trasmissione da ospedale ad ospedale, creando una interconnessione più agile all'interno, ma non solo, della stessa regione, fornendo così un concreto supporto, moderno ed efficace, alle quotidiane attività di sia tipo sanitario che amministrativo.

Seguono le parole di commento: *"Eppure tutto ciò, fino a questo momento, rimane qualcosa di assolutamente non realizzato e non utilizzato. Si immagini il restare nella impossibilità di poter visualizzare le immagini di un paziente che ha fatto una tac, ad esempio a Vicenza, fintanto che non sia il paziente stesso od i familiari a portare fisicamente il "dischetto", o qualsivoglia supporto rigido, su cui poi poter basare le proprie valutazione mediche. È ovvio quindi che tutti i restanti sistemi di interconnessione siano da sempre risultati largamente più agili ed efficaci, da qui il loro abitudinario utilizzo"*.

Preciso istante in cui il colloquio de quo subisce una interruzione, la quale altro non farà che avvalorare, nella maniera più pratica e dimostrativa possibile, quanto detto sin qui, così invero si riprende: *"Ecco una dimostrazione pratica,*

mi è appena arrivato un messaggio tramite whatsapp da parte di un collega, riportante -il paziente X sta sanguinando lo portiamo o meno in sala ?- Certo è indicato solo il cognome, senza nome e senza data di nascita, con la patologia di riferimento, è ovvio comunque che il paziente sia facilmente identificabile".

Così si continua, in un'ottica di commento: *"Questa è la realtà dei fatti e non è superabile: in una comunicazione all'interno di un medesimo ospedale è stato un collega di un'altra specialità ad informarmi circa la situazione di un paziente ed a pormi di conseguenza domande urgenti su come affrontare la specifica situazione. Sistemi di supporto con fini agevolatori ci saranno in futuro, ma non potranno in alcun modo sostituire una comunicazione come quella che ad oggi avviene abitualmente".*

Ciò che si può ricavare quindi è quasi un muoversi in automatismo, dovuto ad una routinaria abitudine, come anche alla necessità di dover gestire il proprio operato professionale quotidiano, nonostante la mancanza di una piena presa di coscienza e consapevolezza circa il valore sotteso al proprio agire, da qui: *"Sono pienamente convinto del fatto che il collega che mi ha appena inviato tale messaggio non ritenga in alcun modo di aver commesso un errore, nonostante abbia fornito un dato clinico ultrasensibile, riferito ad un paziente identificabile, attraverso uno strumento che non è sicuramente congruo per la tipologia di informazione che viene trasferita".*

Ci si interroga pertanto su quanto possa effettivamente essere estesa la mancanza di cyber-cultura in ambito ospedaliero, i fatti di cronaca sembrano parlare chiaro: una larga parte della intrusioni, violazioni, data breach ed altresì attacchi ransomware sono dovuti, o perlomeno facilitati, all'assenza di nozioni e pratiche base di igiene e sicurezza informatica, si pensi all'utilizzo di password di default o al servirsi di sistemi informatici non correttamente aggiornati.

Di seguito la precisazione fornita in risposta: *"Certo tutte queste tipologie di problemi non competono ad un sanitario, tutt'al più alla Direzione, ossia il centro informatico che ogni ospedale ed ogni ASL presenta, d'altronde io non mi sono mai neanche chiesto se il computer dell'Azienda, che ho qui sulla mia scrivania, sia sufficientemente protetto. Ad esempio è il sistema stesso a chiedermi il cam-*

bio delle password dopo il passare di un tot di tempo, sebbene poi alla fin fine le mie password siano sempre le medesime tre che girano e ricircolano al trascorrere ogni tre mesi. Quindi sì, è possibile che ci sia una superficialità sottesa, come anche una non percezione del rischio reale, ma dirò di più forse anche un po' di arroganza da parte della categoria sanitaria, nel pensare di doversi curare unicamente della salute del paziente e poco importa dell'eventualità che i suoi stessi dati possano effettivamente circolare".

Si intervenga allora sostenendo che sebbene sia intuibile la superficialità che si può dimostrare nei confronti di un'eventuale violazione della privacy, non si può non domandarsi se la sensibilità al rischio malevolo cambi laddove ad essere in pericolo possa essere la stessa salute di un paziente, si pensi ai casi di utilizzo di robot chirurgici: *"In tal caso da clinico ho un interesse al corretto funzionamento dello strumento, al fatto che vi sia una corretta riproduzione del mio input, che il mio feedback visivo sia efficace ed affidabile (ossia con latenze che siano le più basse e ravvicinate possibili), e che dalla interazione robot-paziente non derivi alcun danno biologico. Ciononostante, ciò che vi è fra la console ed il paziente stesso non è un problema di mia competenza, se tra qualche anno infatti verrà attuata una implementazione della telechirurgia la stessa tematica delle intromissioni malevoli sarà sì un problema dei sanitari, ma non verrà percepito come tale".*

Rimanendo ancora all'interno del capiente "termine ombrello" dell'e-Health si consideri la delicatezza che può attorniare i sistemi di telemonitoraggio: *"Più attuale e differente risulta tale ambito, siamo infatti dinnanzi ad informazioni che verranno analizzate e utilizzate dal clinico per assumere determinate decisioni, ovvio appare in tal caso l'assunto: se l'informazione fornita è scorretta, il clinico prenderà d'immediata conseguenza decisioni scorrette".* Per esser più chiari si pensi ai casi di telemonitoraggio domiciliare, reso possibile grazie all'utilizzo di dispositivi *wearable* atti a misurare dati quali i parametri vitali di base, col fine di fornire feedback lungo l'arco della giornata relativi ai pazienti, per appurare ad esempio come stia procedendo un post-operatorio.

Così si è voluto puntualizzare: *"Indubbiamente tali dati hanno rilievo, ma importanza ancora maggiore in termini di sicurezza viene rivestita da altre tipologie di*

informazioni e dispostivi - si pensi ai pacemakers o ai defibrillatori impiantabili - anche in questo caso tuttavia la sicurezza verrà data da parte del sanitario per scontata, ossia si confiderà nel fatto che la casa produttrice del dispositivo abbia messo in campo tutta una serie di strategie per far sì che non vi siano intrusioni od altri incidenti".

Si tragga da tali parole una coincisa riflessione: la sicurezza informatica non può ormai esser concepita secondo la classica, ed anacronistica, metafora del "castello", un approccio che ha funzionato in passato finché la maggior parte dei dati ed applicazioni di un'azienda venivano custoditi all'interno di propri data center, protetti in un ristretto perimetro da apposite "cinte murarie" di *firewalls*, piani di *back up,* procedure di gestione degli accessi etc.

Ad oggi infatti il perimetro non risulta più così definito: dati e servizi sanitari raramente appaiono chiusi negli *hardware* delle strutture stesse, viceversa sono sempre più diffusi e scambiati sui *cloud*, si assiste inoltre ad un panorama multisoggettivo (si pensi a tutti i produttori e fornitori terzi di dispositivi, sistemi e servizi), per cui il concetto di sicurezza informatica sta mutando la propria forma verso una nuova effige, ossia quella di una catena. In tale nuovo paradigma è di fondamentale importanza che gli operatori sanitari escano da una logica solista, prendendo maggiore visione d'insieme e coscienza circa la loro appartenenza ad un sistema molto più esteso in cui la propria sicurezza dipende quella altrui e viceversa, solo così non risulteranno essere l'anello debole.

Tornando al colloquio de quo, una volta elencate tutte quelle *capabilities* che paiono esser necessarie al fine di rendere una struttura sanitaria affidabile, efficiente e cyber-resiliente (ossia dalle risorse tecnologiche e strumentazioni mediche adeguate, alle sessioni di *training* e formazione del personale, alla metodologia di gestione del rischio, fino alla compliance normativa nelle nomine di figure quali il DPO, il CISO, od anche il *risk manager*), ci si è domandati se suddetti requisiti vengano concretamente soddisfatti.

A seguire le parole di commento: *"Nelle aziende sanitarie quanto elencato risulta essere presente, sebbene con diversi gradi e complessità, si guardi per esemplificare alla formazione: i corsi che noi sanitari abbiamo come obbligatori da segui-*

re online sono per lo più incentrati proprio sul risk management, od in generale sulle tematiche relative sicurezza, il problema ancora una volta risulta perciò essere alla base. O meglio, è una questione di percezione, capita infatti che per il clinico puro tali tipologie di corsi siano avvertiti quasi come perdite di tempo, ossia quali gravose lungaggini ed inevitabili coercizioni, sebbene possa capitare che le nozioni acquisite risultino anche concretamente utili in occasioni future. Di conseguenza ritengo che sia la trasmissione dell'informazione a dover essere veicolata in una maniera, benché non saprei come, più stimolante ed allettante per il clinico, cosicché non sia percepita quale rigida imposizione".

D'altronde si ritorna di nuovo a rimarcare quell'ottica individualista, solista ed un poco boriosa che sembra alle volte appartenere alla categoria sanitaria: *"in effetti il ragionamento dietro spesso è questo: il mio mestiere è altra cosa, ed è di una nobiltà tale per cui di tutti questi elementi non me ne devo né curare né preoccupare".*

Paiono ad ogni modo parimenti giuste, ragionevoli e ben spese anche le osservazioni poste a difesa: *"noi sanitari siamo soverchiati da problematiche di ordine generale, clinico ed amministrativo, dobbiamo studiare le leggi per la somministrazioni dei farmaci, per i piani di cura, ed ancora dobbiamo spendere dai dieci ai quindici minuti di tempo solo per inserire in maniera digitale la somministrazione del farmaco, per poi controllarla e vigilarla. Quindi si immagini la volontà, e voglia, di dedicarsi anche agli aspetti più propriamente inerenti alla sicurezza dei dati, alle possibili intromissioni ed alla cybersecurity in generale".*

Ed è in questo momento che traspare maggiormente il forte sovraccarico che un clinico può sentir pesare gravosamente su di sé: *"chi si occupa di igiene e prevenzione vuole che io sia formato ed informato sulla sicurezza nel luogo del lavoro, chi invece si occupa di gas biomedicali vuole a sua volta che io sia informato sull'uso delle apparecchiature, chi si occupa di ingegneria, ed io devo utilizzare un elettrobisturi, mi chiede di esser informato sulla sua impostazione e su cosa si debba intendere per un malfunzionamento, dando ovviamente per scontato che, a ben vedere, io dovrò essere assolutamente e perfettamente informato circa la patologia che sto trattando, il paziente che ho dinnanzi ed il suo specifico trattamento".*

Viene pertanto da pensare che vi sia la forte esigenza di formare nuove figure professionali con competenze altamente specifiche e multidisciplinari che debbano essere inserite nell'organico sanitario al fine di affiancare gli operatori stessi e garantire per loro, attenuando in tal modo tutta una serie di incombenze d'organizzazione, amministrative, nonché di sicurezza di cui si trovano ad esser addossati: *"non sto chiedendo che qualcuno mandi e-mail al posto mio, ma che io possa avere ad esempio un sistema di messaggistica imposto dall'Ordine dei Medici che risulti assolutamente blindato."*

Questo non significa deresponsabilizzare l'intera categoria, ma trovare un corretto equilibrio fra le diverse figure che possa risultare ottimale, da qui: *"Noi dobbiamo ovviamente avere chiari i problemi relativi alla cybersecurity, ma dobbiamo parimenti aver chiaro che ci sia qualcuno che quel problema lo può risolvere e lo ha risolto. L'equilibrio sta tutto qui: il problema sì lo dobbiamo conoscere, ma non ce ne dobbiamo concretamente occupare dal momento che non abbiamo tempo, voglia, testa e tantomeno formazione in materia."*

Son parole queste ultime dotate di estrema lucidità ed obiettività, tramite le quali un clinico riconosce la giustezza dell'informarsi, aggiornarsi, e curarsi circa le nuove tematiche emergenti, che siano anche le più lontane possibili dal suo quotidiano operare, ma ugualmente riconosce i propri limiti: *"figure terze devono ad oggi poterci mettere nella condizione migliore affinché i problemi di cyber-sicurezza in primis siano solo più questioni da dover conoscere e non più di cui doverci concretamente occupare"*.

5.5 Intervista: nell'ottica di un ingegnere informatico

Si voglia ora interfacciarsi con la proverbiale "altra faccia della medaglia", costituita dal quel settore professionale legato propriamente alla cybersicurezza ospedaliera, ed in particolare riportando il parere di un ingegnere informatico inserito a pieno titolo in una Azienda sanitaria, al fine di ricostruire un panorama di figure, ruoli e percezioni che appaia il più completo possibile.

Pur riconoscendo che diversi gradi di complessità e eterogeneità possono contraddistinguere l'assetto di ogni struttura ospedaliera, si chieda innanzitutto di tratteggiare l'organigramma di ruoli e figure professionali che orbitano attorno all'ambito della sicurezza, da qui la risposta:

"Per tutte le questioni inerenti alla gestione della privacy si guarda al ruolo dei DPO, ma ciò che più mi compete, e di conseguenza maggiormente conosco, è proprio la disciplina settoriale della security informatica. Quest'ultima, badi bene, è purtroppo una branca molto giovane nelle strutture ospedaliere come quella in cui opero, dal momento che l'attenzione e sensibilità verso tale ambito si è raggiunta solo di recente, proprio in seguito all'inasprirsi degli attacchi informatici ed all'interesse mediatico che ne è conseguito, da tale enfasi ne sono poi scaturiti diversi investimenti in tal senso. Penso di poter dire dunque che solo da un anno a questa parte si è effettivamente posto l'accento sulla security, grazie anche al recepimento della direttiva NIS, per il cui adeguamento stiamo lavorando aspramente, prima di ciò si guardava essenzialmente a quanto previsto dal GDPR in tema di trattamento dei dati personali.

Si domandi pertanto quale sia il panorama normativo di riferimento in tema di sicurezza informatica, se vi siano ulteriori normative o protocolli di settore a cui riferirsi nel proprio operare: "Attualmente la normativa a cui ci riferiamo ed andiamo ad attuare è fondamentalmente la NIS, è il nostro punto focale e filone principale, nonché leva per chiedere finanziamenti ed investimenti che, capirà, in aziende come la nostra, con 50.000 prese di rete e 7.000 dipendenti, sono piuttosto elevati e per nulla banali, e comunque in passato spesso sono venuti a mancare. Nell'ultimo anno invece sono stati stanziati investimenti importanti e questo lascia ben sperare in una direzione di possibile progredimento.

Addentrandosi più specificatamente rispetto al tema delle cyber minacce, si chieda un commento circa i noti fattori di vulnerabilità riguardanti una struttura critica come quella ospedaliera, fra cui l'essere dotati di un sistema informatico complesso, l'utilizzo di dispostivi IoMT non sempre progettati seguendo elevati standard di sicurezza by design, l'articolata catena della supply chain, nonché il fattore umano cui si faccia affidamento, la risposta: "Dunque per tutto ciò che riguarda le tematiche propriamente legate all'IT, quale nostro perimetro storico,

attualmente stiamo portando avanti progetti che paiono essere promettenti, per tutto ciò che attiene invece agli altri ambiti ci atteniamo a quanto ci viene fornito. Mi spiego meglio: i device elettromedicali per loro natura sono certificati CE tout court (cioè per le componenti hardware, software, di configurazione etc.), quindi se noi volessimo installarci un antivirus non è detto che questo sia possibile, dal momento che si va ad inficiare la certificazione stessa. Per riuscire a sopperire a tale problema si è dovuta elaborare una struttura di «securizzazione laterale», in cui i device medicali raffigurano il nucleo, da proteggere tramite cinta murarie di sicurezza, affinché il perimetro sia il meno vulnerabile possibile.

Come vede dunque la tecnologia ci viene in soccorso, però è proprio qui che scatta il terzo fattore, ossia quello propriamente umano, chiaro è che se vedi una postazione di lavoro con una presa USB libera e scarichi i compiti di tuo figlio nel sistema, puoi anche inficiare e far crollare tutto il lavoro che è stato fatto. Vorrei che lei notasse come la parte umana rimanga ad oggi questione davvero rilevante della problematica, veda il dilagante fenomeno del phishing"

Appare lampante la sovrapponibilità di suddette dichiarazioni con quanto dichiarato in precedenza disquisendo con un clinico puro, si ricordi invero come si fosse già confermato l'utilizzo abituale di applicazioni di messaggistica non congrue al trattamento di dati ultrasensibili come possono essere quelli sanitari, si chieda ivi conferma: "È assolutamente così, c'è una totale sconsideratezza nell'inviare referti ed analisi tramite WeTransfer o simili, e ciò è tutt'altro che infrequente, anzi è una pratica comune. Per questa ragione stiamo sempre più insistendo nell'ottica di una maggiore sensibilizzazione ed acculturamento, ad esempio tramite campagne di falso phishing, inviando cioè una serie di email e laddove l'operatore sanitario apra il link, contenente tanto per capirci «bravo hai vinto un milione di euro», riveliamo di esserci noi informatici dalla parte opposta, avvertendo gli operatori stessi che un'azione del genere avrebbe portato a tutta una serie di determinate conseguenze dannose.

Il fattore umano è dunque altamente impattante in una struttura come la nostra e peraltro vorrei far notare come ci siano molte persone estremamente refrattarie al cambiamento delle proprie (scorrette) abitudini operative."

Si voglia ancora ricordare come nell'ottica del clinico puro gli stessi corsi di formazione sui temi della cybersicurezza siano spesso percepiti come gravose lungaggini, da dover seguire solo perché obbligati, segue la veloce interruzione: *"Sì mi lasci dire che la percezione è che la security sia proprio una gran rottura di scatole, intendendola cioè quasi come una limitazione alla libertà personale, vuoi perché non puoi navigare in Internet a tuo piacimento, ma nei siti indicati, vuoi perché non puoi trasferire su WeTransfer un'immagine clinica per avere un secondo parere medico"*.

Chiaro è però come vi sia una costante tensione ed un difficile equilibrio da delineare fra la cura propriamente clinica, anche emergenziale, del paziente e la "cura" degli aspetti maggiormente di privacy e security: *"Esatto, questo è proprio uno dei temi su cui spesso ci scontriamo, in quanto limita il nostro operare, ossia poniamo il caso di un chirurgo che necessita, per il bene del paziente, di fare vedere l'immagine di un tumore ad un collega negli Stati Uniti per avere una seconda opinion, ovvio è che la questione sia altamente delicata. Se lei mi chiede se esistano regole specifiche e normative atte a fare in modo che un tale trasferimento avvenga in maniera sicura, le rispondo di sì, ma tale tipologia di flussi, come può immaginare, non è certamente gratuito, anzi presenta un costo non indifferente"*.

Tornando al tema della cyber-formazione, si rammenti come nell'ottica del clinico puro si dovessero trovare soluzioni innovative e maggiormente stimolanti per incentivare l'apprendimento di nozioni di igiene informatica, si proponga ivi una possibile organizzazione di incontri in presenza, laddove il metodo online possa apparire alle volte maggiormente sgradito e gravoso, così la risposta: *"Io mi occupo della formazione dai tempi precedenti al Covid, di conseguenza non via web, ma in aula, e le persone che avevo dinnanzi si dividevano in due, anzi almeno tre gruppi: gli annoiati, ossia coloro a cui la tematica non importava affatto, che erano presenti solo perché ciò è dovuto, poi una minimissima parte effettivamente interessata all'argomento, e da ultimo una buona parte refrattaria al cambiamento, irremovibilmente radicati ed attaccati alle proprie abitudini, che non sono assolutamente intenzionati a modificare e correggere. Ora addirittura via web non ho nemmeno più questa percezione, basta spegnere la telecamera ed addormentarsi"*.

A seguire vengono pronunciate parole che richiamano alla memoria quella arroganza già ammessa espressamente da parte del clinico: *"Se devo essere sincero, poi sarà una mia percezione soggettiva, c'è proprio un sentimento di superiorità da parte della classe medica, nel pensare di essere in un ambiente prettamente clinico, in cui il core business è la cura del paziente e tutto quanto il resto dovrà essere assoggettato e seguire le esigenze proprie di tale categoria professionale. Non mi spingo oltre, ma comunque tenga presente che io tutti i giorni ho dei disguidi dovuti proprio ai motivi detti fino ad ora"*.

Appare ad ogni modo irrazionale tale ritrosia al cambiamento, soprattutto davanti ad una cybercriminaltà che è in continua crescita, sempre più sofisticata ed invasiva, che non si ferma più solo sul versante della violazione e furto dati, ma che prende di mira le stesse strutture (si pensi agli attacchi ransomware) o che s'introduce nelle apparecchiature e dispositivi, si commenta: *"Per quanto riguarda le intrusioni cyber devo fare un premessa: la telechirurgia deve ancora fare notevoli passi avanti, ad esempio i telerobot utilizzati nella nostra struttura sono utilizzati solo localmente, il paziente ed il robot si trovano cioè a due metri di distanza dall'operatore chirurgico, ed è una modalità operatoria utilizzata più che altro per annullare eventuali tremori fisiologici ed affaticamenti delle braccia del chirurgo, di conseguenza i problemi legati alle intrusioni malevoli saranno eventualmente preoccupazioni future, che seguiranno di pari passo l'evoluzione della medesima telechirurgia.*

Più rilevante invece, quale perimetro che ad oggi nessuno sta prendendo seriamente in considerazione, risulta essere quello dell'attuazione meccanica di dispositivi quali le UTA (unità trattamento aria) [317] *ad esempio usate nelle sale operatorie. Dal mio punto di vista di ingegnere informatico, con una conoscenza di elettronica, io mi preoccuperei di tali sistemi, dato che sono comandati da un sistema informatico IP, banalmente se un attaccante riesce ad intromettersi può manipolarle a proprio piacimento, agire sugli interruttori, arrivando anche a fare saltare la corrente di tutto l'ospedale.*

---

317 Con l'espressione UTA si intendono quelle apparecchiature atte a sopperire alla necessità di mantenere sotto controllo parametri d'aria come umidità, temperatura e purezza all'interno degli ambienti chiusi.

Ecco che il passaggio da un attacco ransowmare diretto a cifrare i dati e chiedere un riscatto, ad un attacco di mera "guerriglia" indirizzato a creare una magnitudo massima di dannosità, pare piuttosto breve. Chiaro che nel secondo caso una volta che il sistema è stato «bruciato» tutto, i paziente attaccati ad un respiratore muoiono, o soffrono comunque un pesante disservizio. Quindi sì, fra le minacce temute da una azienda come la nostra, un posto è senza dubbio rivestito dal ransomware, ma non escluderei possibili attacchi alle UTA od alle cabine elettriche a fini puramente distruttivi. Qui si inserisce la normativa, che per quanto riguarda le UTA prevede che possano essere aperte o chiuse, ad esempio in funzione di un incendio, «anche» per via informatica, bene allora io mi aspetterò che venga studiata, attuata ed implementata «anche» una security informatica in tale direzione.

Procedendo nella discussione si cerchino di riassumere le *capabilities* da adottare affinché una infrastruttura critica sia resiliente ed in grado di mitigare il rischio cyber: risorse tecnologiche adeguate, compliance normativa, sessioni di training del personale, metodologie di analisi e gestione del rischio, strategie di *business continuity e disaster recovery,* periodici test sulla sicurezza dei *device* e soluzione di *identity management* (quali gestione dei privilegi, autenticazioni multifattoriali etc.), da qui il commento: *"In effetti la normativa NIS prevede tutto questo, e ci stiamo attualmente adoperando affinché tali azioni vengano attuate, cercando di sopperire a ciò in cui siamo carenti, il vantaggio apportato dalla NIS è invero l'aver fatto chiarezza sulla strada da dover intraprendere. Non è che prima della NIS non ci fossero buone pratiche adottate, erano tuttavia procedure non scritte, diciamo «tramandate», che a seguire sono state poi specificatamente delineate dalla normativa, che ha avuto peraltro anche il ruolo fondamentale di spostare i riflettori sull'importanza di tali tematiche".*

Si domandi di conseguenza quali siano le sfide attuali od altresì gli ambiti su cui doversi focalizzare al fine di implementare gli attuali livelli di sicurezza: *"A parer mio il fattore umano, inteso dalla base al vertice, ossia dall'operatore utilizzatore della specifica tecnologia alla Direzione stessa, rimane devastante, e necessita ad oggi di un'alta sensibilizzazione sui requisiti di security da dover rispettare.*

Non è più il tempo di una formazione generale e dispersiva, ognuno dovrà essere

istruito in misura settoriale sulle proprie competenze: chi compra device ed apparecchiature, o altresì chi fornisce la struttura, tutti possono a loro modo essere impattanti sulla sicurezza della struttura nel suo complesso.

A me personalmente come formula da seguire piace molto il concetto di cybersecurity "by design", da attuare in tutti i campi, ciò significa che se devo comprare una qualsiasi strumentazione, dovrò richiedere fin dal principio agli stessi fornitori il rispetto di tutta una serie di requisiti di compliance".

Parole conclusive sono state spese in uno spontaneo commento circa lo stato del proprio settore professionale: *"Vorrei comunque ancora sottolineare come i professionisti della security si stiano facendo solamente adesso, difatti persone della mia generazione orientate in maniera specifica e verticale su tali tematiche sono davvero poche. C'è l'attuale bisogno di formare una classe professionale che svolga il mio stesso lavoro, che abbia le spalle un po' più large, seguendo un'ottica diciamo sempre più «entreprise» ed in Italia sotto questo profilo non siamo tanto avanti."*

CAPITOLO 6

LA PREDIZIONE: UN APPROCCIO RISK BASED

6.1 La matrice di rischio

Nei previ capitoli si è avuto modo di comprendere come il *cyber risk* sia ad oggi un rischio che, in certi settori e per alcune tipologie di danni (quali il furto di dati personali, il blocco di attività produttive o catene di fornitura, la violazione sistematica della privacy etc.), possa comportare impatti catastrofali. Pertanto sarà necessario per costruire un'efficace politica di sicurezza,[318] nonché per mettere in atto con successo le strategie preventive sopra descritte, attuare la c.d. "gestione dei rischi" (anche *risk management*), [319] quale processo comprendente tutte quelle azioni finalizzate ad identificare eventuali minacce o vulnerabilità cui una azienda risulti esposta al fine di sviluppare strategie e contromisure atte a poterle mitigare e controllare.[320] Sebbene nessun sistema possa definirsi del tutto sicuro, esiste tuttavia un livello accettabile di sicurezza che è generato proprio dal bilanciamento di varie componenti: il valore di quanto si intende difendere, l'investimento economico che si è disposti a sostenere ed il livello di rischio che si è disposti a tollerare, pertanto risulterà essenziale addivenire ad un ragionevole compromesso tra tali esigenze poste in gioco.[321]

Soffermandosi il tempo dovuto sul concetto stesso di rischio, esso si figura quale condizione esistenziale, ineliminabile di ogni azienda, un fenomeno dalla natura sistematica,[322] che assume carattere dinamico,[323] essendo in grado di influenzare le condizioni di equilibrio economico, finanziario e patrimoniale.

---

318 Per politica di sicurezza si intende la dichiarazione formale delle regole che vincolano coloro che hanno accesso agli investimenti tecnologici e di informazione di un'organizzazione, Cfr. B. Fraser, *RFC2196 : Site Security Handbook*, RFC Editor, USA, 1997.

319 L'emersione della gestione del rischio quale vera e propria disciplina si registra dall'inizio degli anni Cinquanta, in principio tuttavia si rivolgeva quasi esclusivamente all'ambito bancario ed assicurativo, occupandosi dei rischi finanziari (c.d. *insurance risk management*), per poi solo successivamente essere applicata anche in aziende operanti in altri settori, da qui si è avvertita la necessità di istituire all'interno delle imprese una funzione unicamente dedicata a tale attività.

320 C. Zagaria, *L'enterprise Risk Management: gestione del rischio, profili di comunicazione ed evidenze empiriche,* Giappichelli Editore, Torino, 2017, pp. 2-5.

321 L. Donati, G. Vaciago, *Compliance 231: Modelli organizzativi e OdV tra prassi applicative ed esperienze di settore,* Gruppo Sole 24 Ore, Milano, 2022, p. 196.

322 Il primo studioso italiano ad evidenziare la sistematicità dei rischi d'impresa è stato S. Sassi, *Il sistema dei rischi d'impresa,* Vallardi Editore, Milano, 1940, p. 103

323 U. Bertini, Introduzione allo studio dei rischi nell'economia aziendale, Giuffrè Editore, Milano, 1987, pp. 34-35.

Ancora si potrebbe qualificare come l'incertezza misurabile, riferendosi ad eventi, esterni od interni, per i quali è sempre possibile quantificare la frequenza con cui essi sono avvenuti in passato e di conseguenza il grado di probabilità di una loro verificazione futura.

Dando uno sguardo al panorama normativo ed in particolare all'art. 2 del D.lgs. n. 81/2008 (Testo unico per la sicurezza sul lavoro),[324] il rischio viene indicato come *"la probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione"*, si sta pertanto trattando ivi di una grandezza aleatoria, quale esprimente la probabilità che si verifichi un evento in grado di causare concretamente un danno.

Nonostante il legislatore stesso non suggerisca metodologie precise per addivenire ad un preciso calcolo del rischio, nella maggioranza dei casi ci si rifà al c.d. "metodo a matrici", derivante originariamente dalle linee guida Ue atte a indirizzare ed accompagnare piccole e medie imprese verso una corretta ed efficace valutazione dei rischi.

Ebbene la matrice di rischio (anche matrice di impatto), quale strumento di analisi è riassumibile nella formula: [R] = [P] x [E], dove la grandezza [P] suole indicare la quantificazione (stima) della probabilità che il danno, derivante da un fattore di rischio dato, effettivamente si verifichi, mentre [E] risulta essere la quantificazione (stima) del potenziale danno, nella sua entità (o gravità).

La probabilità di accadimento [P] può assumere un valore sintetico in una scala da 1 a 4, a seconda della gamma di soglie di probabilità:

- **[P1] improbabile:** il danno dipenderebbe da una concatenazione di eventi altamente improbabili e fra loro indipendenti, non sono mai stati registrati episodi simili in passato;
- **[P2] poco probabile:** il danno si potrebbe verificare solo in cir-

---

324 Decreto legislativo 9 Aprile 2008 n. 81, *Testo unico in materia di tutela della salute e della sicurezza,* per come aggiornato dalla L. 17 Dicembre 2021, n. 215.

costanze alquanto particolari, raramente simili episodi sono accaduti in precedenza;

- **[P3] probabile:** il danno potrebbe accadere, anche se non in modo automatico o diretto, suscitando una scarsa sorpresa, sono invero già stati riscontrati alcuni episodi simili in passato;
- **[P4] molto probabile:** la situazione rilevata è direttamente correlata al verificarsi di un danno, la cui verificazione non susciterebbe stupore (anzi l'evento sarebbe largamente atteso), sono noti svariati episodi della stessa tipologia accaduti in precedenza.

La gravità del possibile danno [E] può assumere un valore sintetico in una scala da 1 a 4, a seconda della gamma di soglie del danno:

- **[E1] lieve:** si pensi ad un infortunio con effetti di inabilità temporanea, che siano rapidamente reversibili;
- **[E2] significativo:** quale un infortunio con lesioni significative, ma ad ogni modo reversibili a medio termine;
- **[E3] grave:** si pensi ad un infortunio con lesioni significative irreversibili o di invalidità parziale;
- **[E4] gravissimo:** come un infortunio con lesioni altamente gravi irreversibili, invalidità totale o conseguenze letali. [325]

---

325 Si provino a prendere in considerazione i possibili livelli di impatto di un *data breach* (violazione di dati personali), anch'essi infatti saranno distinguibili in: *low* (gli interessati non incontreranno inconvenienti o comunque di poco conto, quale un maggior tempo impiegato a reinserire informazioni); *medium* (gli interessati potrebbero incontrare inconvenienti significativi che saranno comunque in grado di superare nonostante alcune difficoltà, come costi aggiuntivi sopportati); *high* (gli interessati potrebbero incontrare conseguenze significative che dovrebbero esser in grado di superare, anche se sopportando gravi difficoltà, quali danni alla proprietà, peggioramento della salute etc.); *very high* (gli interessati potrebbero incontrare conseguenze significative od addirittura irreversibili non superabili, quali incapacità al lavoro, disturbi fisici o psicologici a lungo termine etc.). Cfr. ENISA, *Online platform for security of personal data processing: reinforcing trust and security in the area of electronic communications and online services,* European Union Agency for Cybersecurity, 19 December 2019, reperibile al sito internet https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform

Pertanto una volta individuata una specifica situazione di pericolo, il valore numerico del rischio [R] sarà stimato quale prodotto fra l'entità del danno [E] e la probabilità di accadimento dello stesso [P], arrivando ad assumere un valore sintetico numerico compreso fra 1 e 16, per come si è voluto ricostruire nella matrice di rischio riportata a seguire:

RISCHIO [R]	Improbabile [P1]	Poco probabile [P2]	Probabile [P3]	Molto probabile [P4]
Danno lieve [E1]	Rischio basso [P1]X[E1]=1	Rischio basso [P2]X[E1]=2	Rischio moderato [P3]X[E1]=3	Rischio moderato [P4]X[E1]=4
Danno significativo [E2]	Rischio basso [P1]X[E2]=2	Rischio moderato [P2]X[E2]=4	Rischio medio [P3]X[E2]=6	Rischio rilevante [P4]X[E2]=8
Danno grave [E3]	Rischio moderato [P1]X[E3]=3	Rischio medio [P2]X[E3]=6	Rischio rilevante [P3]X[E3]=9	Rischio alto [P4]X[E3]=12
Danno gravissimo [E4]	Rischio moderato [P1]X[E4]=4	Rischio rilevante [P2]X[E4]=8	Rischio alto [P3]X[E4]=12	Rischio alto [P4]X[E4]=16

Fig 6.1 Matrice di rischio secondo la formula [R]= [P] x [E]

In definitiva, l'anzidetta matrice risulta schematicamente una griglia, al cui interno da un alto verrà riportata la probabilità che un certo evento si verifichi e dall'altro l'impatto che questo stesso può comportare, incrociando le suddette grandezze poi si otterranno, come possibili risultati, differenti livelli di rischio: [326]

- **Rischio basso [1 ≤ R ≤ 2]:** è da ritenersi pienamente accettabile, sicché non si richiederà l'adozione di alcuna tipologia di intervento;

326 N. Distefano, "Risk Management e Metodi di Risk Assessment: Tecniche per la valutazione del rischio", presentazione presso DICAR (Dipartimento di Ingegneria Civile e Architettura), in data 2 Luglio 2020.

- **Rischio moderato [3 ≤ R ≤ 4]:** è anch'esso sopportabile, per cui l'adozione di specifiche azioni correttive sarà da valutare caso per caso;
- **Rischio medio [R=6]:** è un livello che deve allertare, pertanto occorre tenerlo sotto adeguato controllo, saranno poi necessari interventi tecnici, organizzativi o procedurali, da programmare nel medio termine;
- **Rischio rilevante [R=9]:** non risulta accettabile, richiederà pertanto interventi in tempi celeri atti a risolvere il problema;
- **Rischio alto [12 ≤ R ≤ 16]:** è un livello di rischio assolutamente non accettabile che richiederà di interrompere immediatamente le operazioni e/o le attività e di non riprenderle fintanto che non si sia risolto il problema all'origine.[327]

Sulla base dei risultati sopra ottenuti, saranno adottabili tutta una serie di decisioni, quali: assumersi od evitare il rischio (ad esempio decidendo di iniziare o meno una determinata attività), rimuovere la fonte di rischio (quale una falla nella sicurezza di un sistema), modificarne la probabilità e le conseguenze (adottando misure, strategie e meccanismi di sicurezza), od altresì condividere il rischio stesso (servendosi di servizi assicurativi).

Da ultimo, con l'applicazione di una delle anzidette condotte si andrà ad evidenziare il grado di probabilità e gravità che permarrà, nonostante le azioni di mitigazione poste in essere, ossia il cosiddetto "rischio residuo", che dovrà necessariamente esser tracciato, nonché sottoposto a periodici monitoraggi, in quello che si figura essere un modello di analisi dinamico e circolare.

---

327 ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches,* European Union Agency for Network and Information Security (ENISA), Working document V. 10, December 2013, pp 4-6.

6.2 Valutazione d'impatto (DPIA)

Passando ora a prendere in considerazione l'ambito della salute, risulta chiaro come medici, e strutture sanitarie in generale, debbano anch'essi gestire tutti quei rischi derivanti dal trattamento di una ingente mole di dati ipersensibili dei pazienti, optando per soluzioni operative che offrano massima protezione e riservatezza, nel rispetto dei diritti fondamentali degli individui.

Si ricordi come il Regolamento Ue 2016/679 (GDPR) si muova in un'ottica di responsabilizzazione (o *accountability*) nei confronti della figura del Titolare del trattamento,[328] che dovrà adottare tutte le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, di varia probabilità e gravità per i diritti e le libertà delle persone, inclusa la protezione, ex art. 5 contro *"trattamenti non autorizzati o illeciti, la perdita, la distruzione o il danno accidentale"*. Ecco come posto di spiccato rilievo viene assunto, tra le novità introdotte dalla suddetta disciplina europea, dalla Valutazione d'impatto sulla protezione dei dati (anche detta DPIA, ossia *Data Protection Impact Assessment*), quale processo volto a descrivere il trattamento, valutarne necessità e proporzionalità, nonché ad identificare e gestire i rischi che ne derivino per i diritti delle persone fisiche, determinando in tal modo tutte le misure e tecniche atte ad affrontarli.

Nello specifico dall'art. 35 del Regolamento Ue, si evince come la DPIA sia obbligatoria laddove si svolgano trattamenti che, per loro stessa natura, oggetto, contesto e finalità possano presentare un rischio considerabile come elevato.[329] Ov-

---

328 Il Titolare del trattamento, ex art. 4 GDPR "*persona, fisica o giuridica, che dispone dei dati e determina i fini e le modalità del trattamento",* nel caso della libera professione in uno studio privato, sarà rinvenuto nella figura del medico. Quest'ultimo può trasmettere certo informazioni ad altri soggetti, si pensi ad un laboratorio esterno di analisi cliniche, che tutt'al più sarà inteso quale Responsabile del trattamento, ossia soggetto esterno, che tratta i dati solo su istruzione del Titolare, privo del potere di iniziativa o di autonomia decisionale. Nella sanità pubblica invece la titolarità dei dati personali che tratta il medico di base è, in linea di principio, in capo alla ASL o ai servizi della Regione, o anche al Ministero della salute. Dunque il medico rivestirà in tal caso la funzione di Responsabile del trattamento, ricevendo istruzioni (e subendo i controlli) da parte di tali strutture.

329 Così recita l'art. 35 Gdpr: *"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".*

vio è come identificare tutti i casi rientranti nello scenario appena delineato non sia sempre un'operazione semplice ed immediata, per questo si necessita di una fase preliminare, definibile per l'appunto come "prevalutazione d'impatto", in cui il titolare del trattamento, una volta raccolte le informazioni essenziali, coadiuvato dal DPO (*Data protection officer*) qualora designato, valuterà l'opportunità e/o la necessità di procedere o meno ad una DPIA. Il GDPR stesso viene in soccorso in tale prevalutazione, non elencando tassativamente i casi di obbligatorietà, ma limitandosi ad individuare tre ipotesi generali in cui la DPIA viene richiesta:

a. quando il trattamento comporta una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b. in caso di trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 (fra i quali, si ricorderà, sono compresi i dati relativi alla salute);

c. qualora il trattamento abbia ad oggetto la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

A tali indicazioni generali poi si vanno a sommare le Linee Guida WP 248 emanate dal Gruppo di lavoro "Articolo 29" (ad oggi *European Data protection Board*), che a loro volta identificano nove casi in presenza dei quali si può desumere che il trattamento presenti proprio *"un rischio elevato per i diritti e le libertà delle persone fisiche"* e che dunque si debba procedere con la DPIA: [330]

a. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione;

b. processo decisionale automatizzato, mirante a consentire

330 Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 re.01, 4 April 2017.

l'adozione di decisioni in merito agli interessati che abbiano effetti giuridici o che incidano in modo analogo significativamente su dette persone fisiche;

c. monitoraggio sistematico;

d. trattamento di dati sensibili od aventi carattere altamente personale;

e. trattamento di dati su larga scala, valutando a tal fine: il numero di soggetti interessati, il volume e le diverse tipologie dei dati, la durata, la persistenza ed altresì la portata geografica dell'attività di trattamento;

f. creazione di corrispondenze o combinazione di insiemi di dati;

g. trattamento di dati relativi ad interessi definibili come vulnerabili;

h. uso innovativo od anche applicazione di nuove soluzioni tecnologiche ed organizzative;

i. quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o contratto.

Risulta evidente come l'ambito sanitario vada a soddisfare molteplici dei suddetti requisiti, dal momento che risulta qualificabile come trattamento "su larga scala" di dati "sensibili" e/o relativi a categorie di interessati "vulnerabili" (si pensi a minori, anziani, pazienti affetti da patologie invalidanti etc.), che fa largo uso di tecnologie "avanzate ed innovative".

Effettivamente la rilevazione di dati e parametri vitali tramite strumenti di monitoraggio a distanza (o mediante *wearable devices*), l'utilizzo di sistemi di AI per l'individuazione di terapie personalizzate, l'adozione di tecniche di *machine learning* nell'individuazione di gruppi di pazienti con una maggiore o minore propensione a sviluppare specifiche patologie, sono tutti esempi di acquisizione di dati che incidono sì principalmente sul diritto alla salute, ma altresì su svariati

ambiti di vita quotidiana dei singoli individui, per tale motivo una valutazione d'impatto incentrata sull'analisi dei rischi derivanti da tali tipologie di trattamenti sanitari si profila come pienamente necessaria. [331]

Uno specifico modello di gestione dei dati dovrà essere in grado infatti di assicurare, costantemente, la riservatezza, l'integrità, la disponibilità ed anche la resilienza dei sistemi, cosicché in caso di accadimento di un evento negativo (interno od esterno) si possa comunque ripristinare tempestivamente tanto la disponibilità quanto l'accesso ai propri dati personali. [332]

Si passino così a considerare le concrete fasi del processo iterativo di una DPIA, per come vengono delineate dalle sopradette linee guida del WP29:

a. Descrizione del trattamento: innanzitutto occorrerà identificare tutti i diversi soggetti che siano coinvolti a diverso titolo (titolare ed eventuali contitolari, *outsourcer* responsabili esterni, amministratori di sistema etc.), come anche le tipologie di dati trattati, le piattaforme tecnologiche utilizzate e le finalità del trattamento stesso.
L'individuazione dei soggetti e la definizione dei livelli di responsabilità è indubbiamente un primo step difficoltoso, considerando la necessaria condivisione ed interoperabilità che caratterizza primi fra tutti i dati sanitari (si pensi a tutti gli episodi sanitari che caratterizzano la presa in carico di un paziente: assistenza domiciliare, programmi di screening,

---

331 Il Considerando 75 del GDPR identifica cosa si debba intendere con il concetto di rischio, riportando che: *"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali […] ".*

332 C. Gallotti, *Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma IOS/IEC 27001*, Lulu Press Inc., Raleigh, 28 Gennaio 2019.

assistenza specialistica ambulatoriale, ricoveri, riabilitazione, gestione della cronicità etc.). Durante ogni contatto infatti il paziente riceve determinate prestazioni (visite, esami, terapie, interventi etc.) che a loro volta ingenerano atti sanitari (un referto, il risultato di un esame di laboratorio etc.) per i quali può essere necessario impiegare risorse (materiali, attrezzature, spazi etc.) e dati clinici, che successivamente potranno essere aggregati e strutturati in documenti più complessi per essere consultati da differenti tipologie di utenti in funzione dei profili di abilitazione e delle differenti esigenze cliniche (percorsi diagnostici, terapeutici, assistenziali etc.).[333] Risulta evidente come, alla luce della particolare sensibilità e rilevanza sia per la sicurezza dei procedimenti che dei pazienti, i dati clinici debbano essere gestiti seguendo criteri di sicurezza e tracciabilità (ossia verificando i sistemi di log management, assicurando l'autenticità, la data certa e le versione dei documenti ed altresì garantendo la loro non cancellazione o sovrascrittura);

b. Valutazione circa la necessità e proporzionalità del trattamento: in tale fase, una volta individuate possibili linee guida di riferimento da seguire (quali in materia di referti online, sul trasporto di campioni diagnostici, sul generale trattamento di dati genetici etc.) e descritto il ciclo di vita dei dati, la valutazione della proporzionalità dovrà essere approfondita in termini di quantità, frequenza, persistenza di raccolta di dati, come anche di ampiezza geografica dell'area di raccolta (si pensi ad un titolare che operi su più presidi territoriali);

c. Valutazione dei rischi: è indubbiamente la fase saliente della DPIA, in cui peraltro si evidenzia la necessità di far sì che

333 P. Locatelli, D. Zacchetti, F. Chiodini, F. Ferrara, "I modelli necessari a strutturare un clinical data repository", in *Progettare per la sanità*, n. 5, Ottobre 2019.

la predisposizione del registro dei trattamenti [334] non sia un mero esercizio forma, ma piuttosto l'esito di una attenta valutazione tanto del contesto organizzativo di riferimento quanto dei processi aziendali da cui le attività di trattamento dei dati scaturiscono. Per una corretta individuazione delle minacce si opererà una combinazione dei seguenti elementi, che stanno all'origine dei possibili incidenti: risorse (hardware, software, infrastrutture, etc.), azioni (guasto, atto doloso, errore etc.) e rischi dati (perdita di integrità, di confidenzialità, di riservatezza etc.). Così a titolo esemplificativo, la minaccia di accesso abusivo ad un sistema è conseguenza di un atto doloso (azione), perpetrata su di una infrastruttura di rete (risorsa) che avrà ripercussioni sulla confidenzialità del dato. Ovvio è che suddetta analisi delle minacce non dovrà essere limitata al mero "rischio dato" inerente alla perdita di integrità, confidenzialità e disponibilità, ma anzi dovrà prendere in considerazione anche i possibili effetti che il rischio può avere per i diritti e le libertà delle persone fisiche, seguendo così un approccio altamente multidisciplinare che tenga conto in egual misura della sicurezza dei pazienti, della continuità operativa, della cybersecurity ed anche della capacità di resilienza dei sistemi. [335]

---

334 Si rammenti come, ex art. 30 Gdpr, suddetto registro altro non sia che lo strumento attraverso il quale il titolare e il responsabile del trattamento documentano in forma scritta, le principali informazioni relative alle attività di trattamento e alle misure di garanzia adottate, in base alle finalità perseguite e ai profili di rischio rilevati, al fine di poter poi dimostrare all'Autorità di controllo (ossia il Garante per la protezione dei dati) di aver adempiuto correttamente al proprio obbligo circa la protezione dei dati personali.

335 Si rimarchi ivi la nozione di *"sicurezza by design":* una adeguata DPIA dovrà essere fatta in fase di concepimento di un servizio, assicurando lo svolgersi di un integrale e corretto processo di sicurezza nell'acquisizione di sistemi e servizi, nella contrattualizzazione con i fornitori, così da sviluppare il *procurement* stesso in un modo sano. In tal modo si può avere una evoluzione dei servizi verso una maggiore resilienza nei confronti degli attacchi, se invece si affrontano tali iter come oneri burocratici, cercando di minimizzare il fastidio che crea la DPIA, a questo punto si perde una fondamentale occasione.

6.3 Capire, valutare e gestire il rischio cyber

A proposito di rischio si rilevi come nel complesso panorama sanitario oltre alla sicurezza delle cure, vi sia quella del farmaco, quella dei luoghi di lavoro, del rischio infettivo, delle radiazioni ionizzanti, quella strutturale ed ovviamente quella informatica. Tutti tali aspetti orbitano attorno a chiunque partecipi alla vita delle aziende sanitarie (si pensi ad operatori, utenti, fornitori terzi, visitatori etc.), ebbene non pare più possibile ragionare "per silos", anzi ad oggi occorre una visione del rischio che sia quanto più integrata e complessiva possibile.

Ad ogni modo sono gli attuali fatti di cronaca a parlare chiaro: l'ambito sanitario risulta uno dei settori maggiormente esposti e vulnerabili sul versante della *cybersecurity*.

Tra i fattori di rischio che più possono incidere in tal senso si notino:

a. L'ampia diversificazione delle figure professionali coinvolte, ognuna di queste con diversi profili di autorizzazione nei sistemi informatici e che spesso si ritrovano a poter accedere anche a più attrezzature collegate in rete;

b. La necessità di garantire l'interoperabilità dei sistemi, e di integrare attrezzature fortemente diversificate sia all'interno della organizzazione che lungo la *supply chain*;

c. L'utilizzo di strumentazioni medicali, fra cui sempre più soluzioni IoMT, non sempre progettate secondo una logica di sicurezza by design e che, non di rado, si ritrovano ad essere dotate di sistemi operativi obsoleti o per i quali non sono facilmente disponibili o reperibili patch di aggiornamento. Ad oggi invero un paziente può essere monitorato in modo più completo, senza tuttavia la necessità di appuntamenti "faccia a faccia" o trattamenti invasivi (si pensi al telemonitoraggio domiciliare attuato tramite dispositivi indossabili). L'attuale molteplicità di dispositivi interconnessi crea numerosi poten-

ziali punti di infiltrazione e conduce inevitabilmente alla possibilità di subire maggiori attacchi informatici.[336] Sotto quest'ultimo profilo si rammenti ivi la c.d. Valutazione delle tecnologie sanitarie (anche detta *Health Technology Assessment o HTA*) quale strumento utilizzato a livello internazionale consistente nella *"complessiva e sistematica valutazione multidisciplinare circa le conseguenze assistenziali, economiche, sociali ed etiche provocate in modo diretto ed indiretto, nel breve e lungo periodo, dalle tecnologie sanitarie esistenti e quelle di nuova introduzione"*.[337]

È dunque una guida, un ponte fra il mondo tecnico-scientifico e quello propriamente decisionale, incentrata sull'analisi delle conseguenze attese dall'introduzione di specifiche tecnologie sanitarie, nonché di soluzioni digitali nel contesto di una organizzazione sanitaria (si pensi all'adozione di nuovi dispositivi medici, farmaci, sistemi diagnostici, procedure chirurgiche, percorsi assistenziali, attrezzature sanitarie, od assetti strutturali, organizzativi e manageriali, etc.), atta a focalizzare l'attenzione sulla attenta valutazione circa i profili di: efficacia clinica, protezione dei dati personali, prospettiva dei pazienti, cybersicurezza, aspetti economici, organizzativi, come anche etici e legali;

d. La stessa mancanza di risorse ingenera vulnerabilità, volendosi riferire sia al fattore umano, per cui il personale IT risulta essere inadeguato, mancando per di più figure altre che possano occuparsi di campi multidisciplinari quali il *risk management*, la *data protection* o la stessa *privacy management* (portando ad una inevitabile ambiguità rispetto a chi sia effettivamente

---

336 D. Farringer, "Maybe if we turn it off and then turn it back on again? Exploring Health Care Reform as a means to curb cyber-attacks", in *Journal of Law, Medicine & Ethics,* 47(S4), 2019, pp. 91-201.

337 Commissione Europea, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla valutazione delle tecnologie sanitarie, che modifica la Direttiva 2011/24/UE, Bruxelles, 31.01.2018; si faccia riferimento anche alla Carta di Trento sulla valutazione dei servi sanitari, quale documento fondante la Società Italiana di Health Technology Assessment,* Trento, in data 28 Marzo 2006.

> responsabile circa le tematiche di sicurezza). Ma un'altra risorsa a mancare risulta essere proprio il *budget* ed uno dei motivi per cui i fondi per la sicurezza informatica sembrano essere insufficienti è che le organizzazione sanitarie tendono ad indirizzare le proprie scelte d'acquisto, nonché finanziamento verso risorse legate propriamente all'assistenza clinica ed alle cure mediche, lasciando gli aspetti legati alla cybersicurezza nel dimenticatoio. [338]

Chiaro risulta come la cultura del rischio si sia evoluta nella sanità italiana, facendosi strada la graduale consapevolezza per cui la sicurezza in sanità non possa limitarsi solo più al rischio clinico, ma debba abbracciare ogni ambito, dall'informatico, al gestionale ed altresì strutturale. Il paradigma invero sta per mutare: dati e servizi sanitari saranno sempre meno chiusi negli *hardware* delle strutture sanitarie e sempre più diffusi e scambiati sui *cloud*, e ciò non farà altro che aumentare i rischi. Occorre dunque cogliere questo momento di passaggio per costruire una matura cultura delle sicurezza cyber prima che sia fin troppo tardi per arginare i danni.

Si voglia indirizzarsi verso le conclusioni riportando di seguito il *survey* realizzato da SHAM Italia, società specializzata in assicurazione e gestione rischi, datato al 2021, quale indagine conoscitiva rivolta ai professionisti ed alle strutture sanitarie e socio-sanitarie italiane, col preciso obiettivo di comprendere quanto il cyber-rischio sia conosciuto, come venga gestito, ed altresì quali siano le prospettive per il futuro. [339] In particolare i partecipanti a tale sondaggio sono stati 68, provenienti da strutture ed aziende sanitarie, pubbliche e private, di 14 regioni italiane, sebbene non si tratti di un campione eccessivamente esteso, il contributo fornisce ad ogni modo un valido punto di partenza per comprendere il grado di consapevolezza degli operatori sanitari su tema del rischio cyber come anche quali

---

338 S. Ghafur, E. Grass, N. R. Jeggings, "The challenges of cybersecurity in health care: the UK National Health service as a case study", in Lancet Digit Health, Volume 1, issue 1, May 2019, pp. 10-12.

339 SHAM ITALIA, *Capire il rischio cyber: il nuovo orizzonte in sanità,* whitepaper SHAM Italia, 2021.

siano le principali aree dove intervenire al fine di poter migliorare il campo della sicurezza informatica.

Il primo dato ricavabile, che lascia peraltro ben sperare, è l'alta sensibilità in materia: circa il 60% dei rispondenti (ossia Referenti di direzione sanitaria generale e di ingegneria clinica, responsabili CISO della sicurezza informatica, Risk manager, Data protection officer etc.) dichiara invero il *cyber risk* come altamente impattante sui modelli organizzativi interni e sulle attività da erogare, oltre ad un ulteriore 31% che lo qualifica comunque come un tema parzialmente prioritario, se si vanno a sommare tali due espressioni di interesse si ottiene un buon 90% dei rispondenti che valorizzano positivamente l'interessamento al tema de quo.

Di contro però l'immediato paradosso: il 53% dei rispondenti dichiara di non aver (o aver solo in parte) definito concretamente un piano di gestione del rischio, solo il 44% poi dichiara di aver reattivamente adottato ed implementato azioni di miglioramento interno in seguito all'avverarsi di eventi avversi, ed ancora meccanismi quali mappature dei rischi od anche test sulle vulnerabilità risultano scarsamente effettuati (da circa il 30% dei rispondenti).

Ebbene all'elevato interesse sul tema non sembra quindi corrispondere un altrettanto sentita sua identificazione, misurazione e gestione, si noti peraltro come solo il 10% dei rispondenti affermi di aver provveduto a contrarre apposite polizze assicurative contro i danni informatici al fine sia di trasferire eventuali conseguenze economiche circa un evento avverso, sia di avere un adeguato supporto tecnico attivo in caso di necessità. Soffermandosi celermente sui rischi legati alla sottrazione dati ed alla violazione della privacy, è da rilevare come nel corso degli ultimi anni sia cresciuta in maniera esponenziale la domanda di coperture assicurative strutturate in modo da affrontare i costi relativi a tali nuovi rischi ed incidenti cyber. Anche in tali tipologie di polizze si troverà una concezione strettamente attuariale delle assicurazioni, basata sulla capacità di prevedere in anticipo la probabilità e l'impatto di possibili eventi dannosi, informazioni che vengono per lo più ricavate dai dati relativi al passato, facendo poi delle ipotesi sui futuri accadimenti. Ciononostante, suddetti rischi risultano comunque particolarmente complessi da decodificare, a causa proprio della rapida evoluzione tecnologica che caratterizza il settore de quo.

Sicuramente nel novero delle principali cyberminacce per le quali potrebbe essere disponibile una copertura assicurativa rientrano:

a. la divulgazione di informazioni sensibili protette od il blocco dei sistemi informatici (si ricordi come l'estorsione preveda, nella maggior parte dei casi, il pagamento del riscatto tramite valuta digitale);

b. il mancato guadagno lungo il perdurare di un certo periodo di tempo, determinato a causa di un evento di violazione delle informazioni. [340]

Rimane tuttavia importante considerare che sarebbe del tutto irrealistico pensare di poter azzerare completamente il rischio cibernetico all'interno di una azienda: diventa quindi ineludibile un cambio di paradigma, che vede un diretto coinvolgimento ed una forte implementazione del *risk management,* nelle sue diverse declinazioni di: mitigazione, prevenzione, trasferimento ed assunzione del rischio.

Ed il *risk management* dovrà essere inteso quale approccio valutativo che incomincia con l'identificazione di tutti i rischi potenziali, nonché degli asset e delle specifiche vulnerabilità, per successivamente valutare la probabilità circa l'avverarsi di un evento avverso, il suo impatto e le misure di salvaguardia da adottare per ridurne gli effetti negativi. Solo così il rischio potrà essere mitigato ed altresì costantemente monitorato nel tempo, seguendo una procedura dal carattere fortemente circolare atta a garantire alti livelli di cybersicurezza. [341]

---

340 Volendo poi indicare quali siano le coperture assicurative che concernono il c.d. rischio cibernetico si possono individuare due tipologie: l'Assicurazione primaria diretta che risarcisce chi si assicura (per danni ad asset informatici, interruzione dell'attività, danno reputazionale, estorsione, furto, etc.); ed Assicurazione RC vs. terzi (nei casi di violazioni di dati sensibili, spese legali, indennizzi a terzi), Cfr. C. Savino, "Cyber risk, assicurazioni e PMI", presentazione per Ania: Associazione Nazionale fra le imprese assicuratrici, 7 Marzo 2017.

341 S. Bhuyan, U. Kabir, J. M. Escareno, K. Ector, S. Palakodeti, D. Wyant et al., Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations, in *Journal of Medical Systems,* Vol. 44/98, 2 Aprile 2020.

Da qui l'assunto cardine per indirizzare il futuro della sanità italiana: senza una adeguata sicurezza, la digitalizzazione del settore sanitario non potrà mai dispiegarsi compiutamente, in quanto la sicurezza stessa non è una risposta alla innovazione, ma piuttosto il suo requisito fondamentale.

6.4 Una visione d'insieme

Si voglia a questo punto indirizzarsi verso riflessioni conclusive fornendo una prospettiva sistematica e strutturata, volta ad analizzare le dinamiche di sviluppo ed implementazione della *cybersecurity* nelle strutture ospedaliere e su come talune dinamiche organizzative interne possano a tutti gli effetti interagire fra loro al fine di sviluppare un sistema sanitario complessivamente cybersicuro. Si è già ampiamente notato nel discorrere dei capitoli precedenti come le *capabilities* relative alla cybersicurezza in sanità includano una ampia varietà di programmi, sistemi, comportamenti e tecnologie che un ospedale può decidere di impiegare col preciso obiettivo di potenziare la propria resilienza informatica.

Tuttavia non tutte le anzidette strategie e soluzioni operative si presentano come autosufficienti, anzi possono erodersi e scemare nel tempo laddove non vengano opportunamente attuate, adottate, monitorate e mantenute. Al fine di voler riassumere graficamente un panorama organizzativo così complesso si farà uso a seguire delle variabili di stock e di flusso.[342] Si incominci dunque dando uno sguardo al nucleo del modello proposto, ossia la variabile di stock evidenziata e denominata *"Cybersecurity capabilities at hospital"* quale raffigurante l'accumulo di tutti i programmi implementati e comportamenti adottati determinanti la sicurezza complessiva di una specifica organizzazione. Una variabile di flusso invece ha la funzione di modificare e far variare quella anzidetta di stock, da qui si possono notare la variabile di afflusso (*"Cybersecurity capability development"*),

342 Una variabile di stock è misurata in uno specifico momento e rappresenta una quantità esistente in un determinato istante, una variabile di flusso è misurata invece relativamente ad un intervallo di tempo, queste ultime fanno variare le variabili di stock.

indicante il tasso al quale le capacità vengono aggiunte allo stock esistente, e di deflusso (*"Cybersecurity capability erosion"*), specificante viceversa il tasso al quale le capacità stesse vengono eliminate dallo stock esistente (Fig. 6.2). [343]

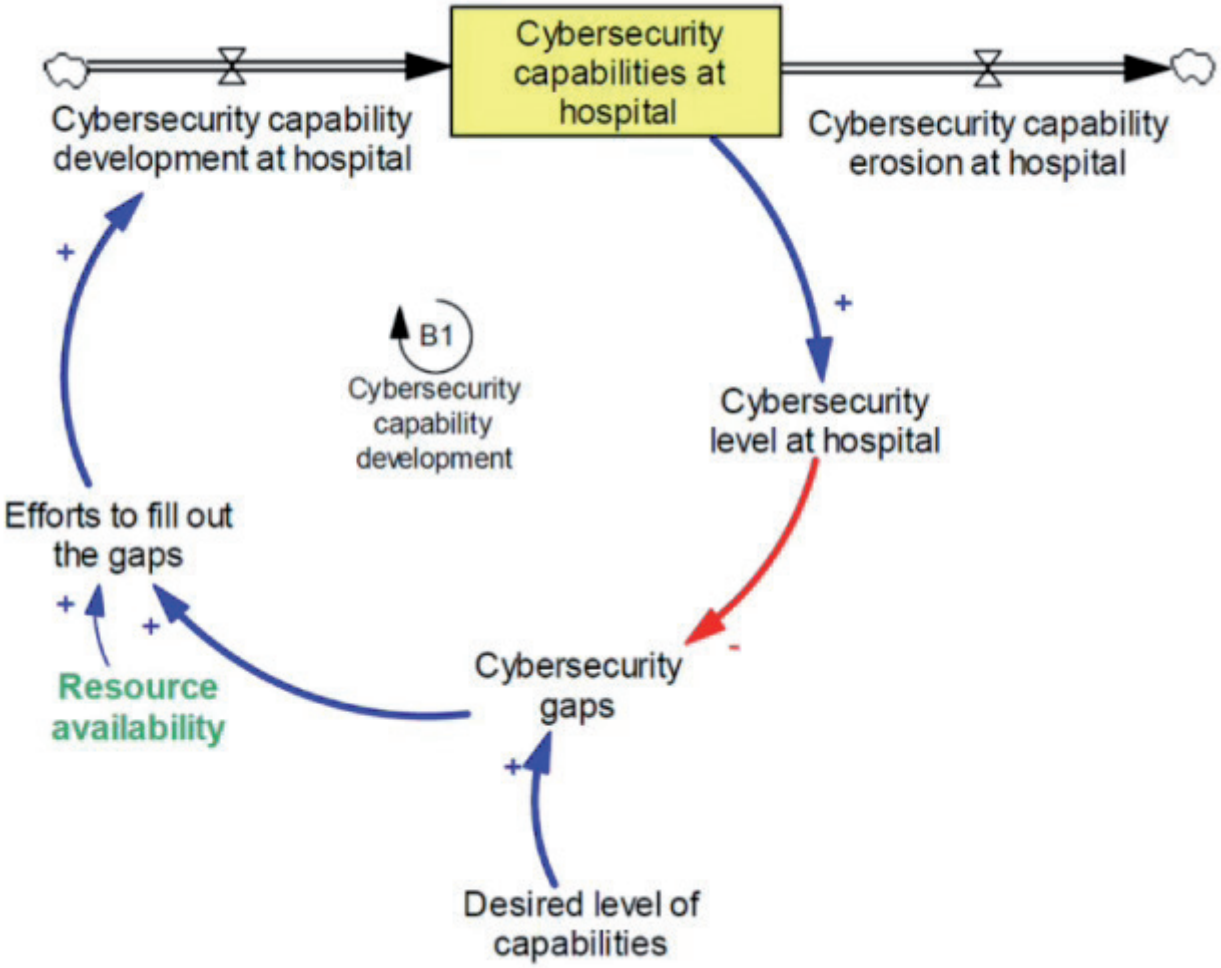

Fig. 6.2 Primo loop di cybersecurity. Fonte: "Cybersecurity in hospitals: a systematic, organizational perspective", in Journal of medical Internet Research, rimando a nota.

Un primo fattore variabile viene rappresentato dalla disponibilità di risorse *("Resource availability"):* mezzi quali acquisti, protocolli, strumenti, tecnologie e perso-

343 M. S. Jalali, J. P Kaiser, "Cybersecurity in hospitals: a systematic, organizational perspective", in Journal of Medical Internet Research, Vol. 20, iss. 5, 2018, pp. 1- 16; si noti come nonostante sia uno studio formulato guardando al sistema sanitario statunitense, tuttavia risulti essere un modello applicabile anche ai sistemi sanitari di altri Paesi.

nale costituiscono invero gli elementi costitutivi essenziali che consentono ad una struttura sanitaria di compiere gli sforzi necessari al fine di aumentare la *capability development rate* e di conseguenza incrementare lo stock delle attuali potenzialità ospedaliere. A sua volta ciò innescherebbe un accrescimento circa il livello di sicurezza informatica *("Cybersecurity level"),* riducendo il divario fra il livello effettivo e quello desiderato di protezione, e, si capirà, laddove tale gap diminuisca, si attenueranno di conseguenza anche gli sforzi *("Efforts to fill out the gaps")* richiesti per colmare le lacune di sistema. È così che si verrà a delineare un primo anello, anche detto feedback loop (B1) indirizzato a bilanciare e stabilizzare il sistema complessivo, guidandolo verso il raggiungimento dell'obiettivo desiderato.

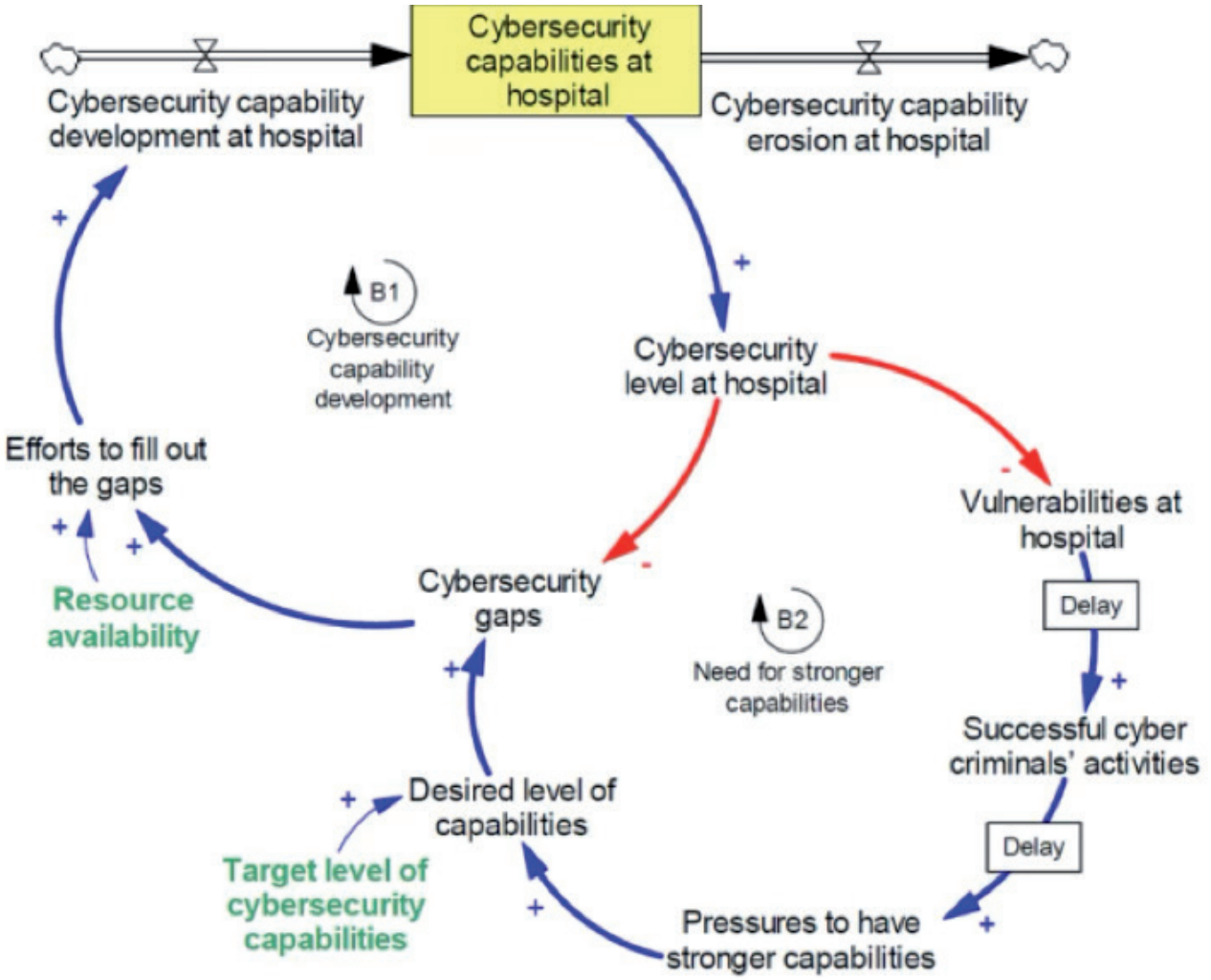

Fig. 6.3 Secondo loop di cybersecurity

Congiungendo allo schema *de quo* ulteriori elementi (Fig. 6.3), si osservi come il livello di sicurezza possa calare a causa della presenza di specifiche vulnerabilità (si pensi all'arretratezza delle tecnologie adoperate), che implicano una più alta probabilità di successo circa la perpetrazione di eventuali cyber attacchi, che laddove raggiungano effettivamente un esito positivo, non faranno altro che sobbarcare una data struttura di maggiore pressione ed impellenza circa l'urgente necessità di raggiungere il livello desiderato (nonché richiesto) di *security* (da qui il secondo cerchio, o *balancing loop* B2, raffigurante il giungere del bisogno di più robuste *capabilities*).

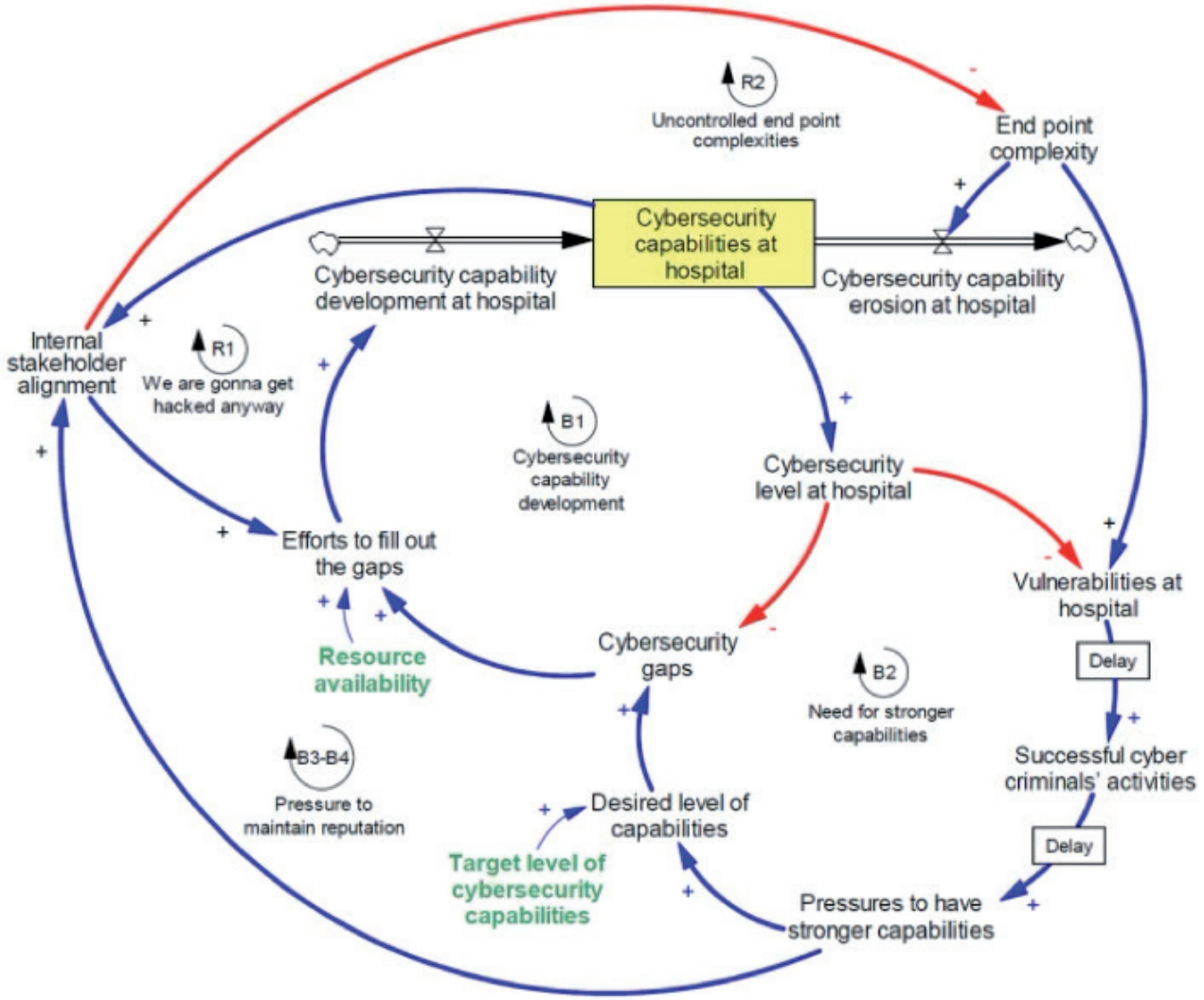

Fig 6.4 End point e stakeholder nel sistema

Ancora si vogliano aggiungere ulteriori fattori rilevanti (Fig 6.4), *in primis* la complessità degli *end point* (ossia di tutti i device, strumenti, apparecchiature e macchinari interconnessi), aggravata dalla mancanza di consapevolezza da parte del personale medico circa le corrette pratiche di sicurezza informatica da dover adottare nell'operare quotidiano, andando così ad accentuare fortemente le già esistenti vulnerabilità della struttura, conducendo inevitabilmente ad una riduzione della complessiva capacità dell'organizzazione di gestire lo scenario relativo alla propria cybersicurezza. *In secundis* si sottolinei come laddove tutti gli attori dell'organigramma sanitario non riconoscano la dovuta importanza alle tematiche di security, cooperando e collaborando fra loro, andranno a minare fortemente tutti gli sforzi fatti per colmare tutte le lacune di sistema sopradette, impattando negativamente sul livello generale di *cybersecurity* (entrando in un loop recitante *"We are gonna get hacked anyway"*).

Viceversa dovrebbe essere proprio quella anzidetta pressione ingenerata dall'eventualità di subire cyber attacchi indirizzati alla propria struttura (quale il non voler subire un danno reputazionale) a spingere tutti gli *stakeholder* interni ad allinearsi lungo la medesima strategia operativa difensiva e di rafforzamento della propria resilienza. Ebbene il meccanismo circolare delineatosi sino a qui non risulta, a ben vedere, applicabile solo ad una singola realtà ospedaliera, ma altresì a tutto un sistema sanitario nella sua interezza, essendo che le vulnerabilità informatiche proprie delle strutture sanitarie in un dato Paese altro non è che il risultato, non certo di una, quanto di una ingente molteplicità di strutture.

Per esemplificare si ipotizzi di applicare il modello *de quo* su 1000 ipotetici ospedali (nonostante ciascuno abbia il proprio livello di disponibilità di risorse ed il proprio personale target di sicurezza da raggiungere), ciò che è ricavabile da suddetta operazione è proprio il livello di vulnerabilità complessivo di un sistema sanitario, che andrà necessariamente a determinare l'attrattiva che quest'ultimo riveste per l'agire di cybercriminali (attrattiva che verrà valutata assieme ad altri fattori variabili, quali il valore economico dei dati sanitari custoditi dalle diverse organizzazioni).

Pertanto guardando i risultati ottenuti adottando un punto di vista macro, la vulnerabilità cyber delle infrastrutture ospedaliere di un dato Paese si ritrova ad esser fortemente condizionata dalle *capabilities* proprie di ogni singola struttura.

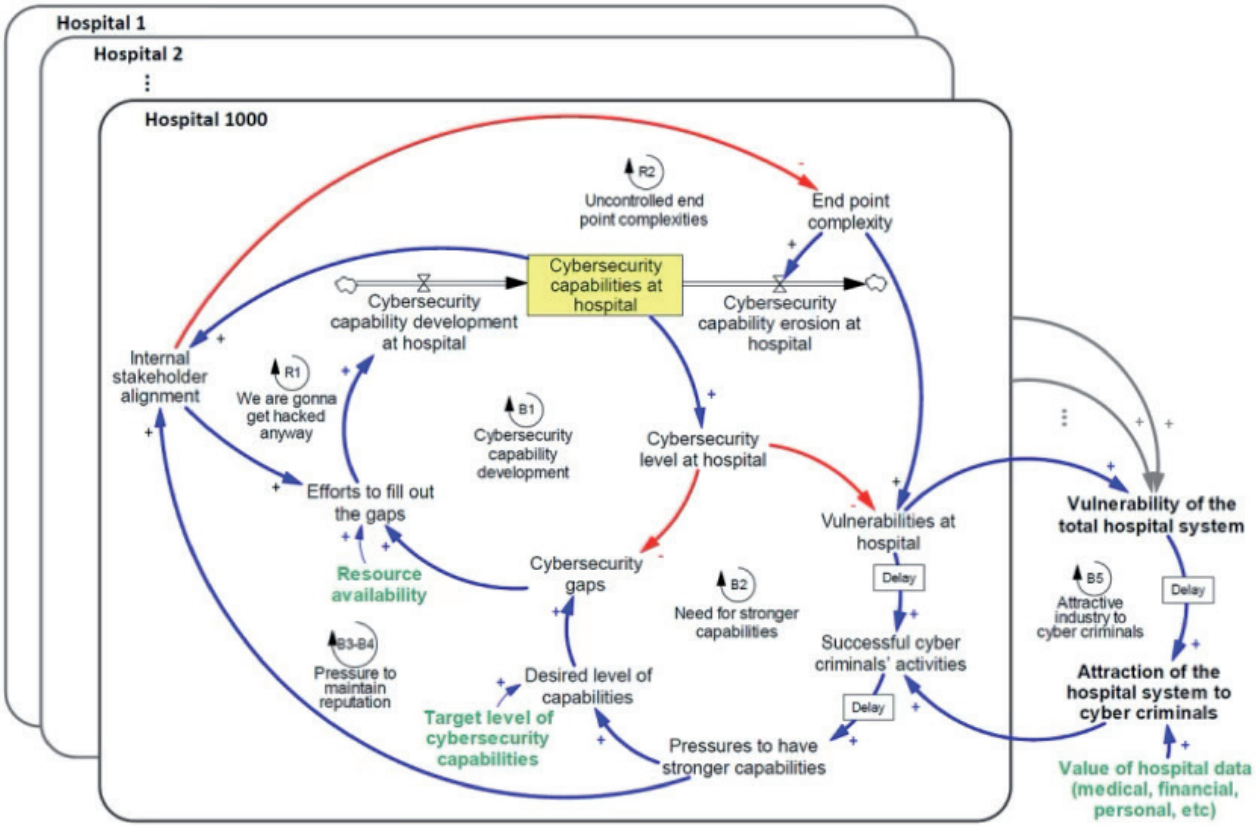

Fig. 6.5 Applicazione del modello su larga scala

Cercare dunque di ridurre ed appianare i divari circa le differenti disponibilità di risorse (tanto fisiche quanto umane) fra diversi ospedali, disseminati in una data zona geografica, potrebbe aiutare a rendere l'intero sistema meno vulnerabile, si spieghi meglio: anche solo pochi ospedali con scarsi livelli di *cybersecurity* potrebbero andare a minare un'intera assistenza sanitaria nazionale. In altre parole risulta ad oggi necessario che le strutture si muovano unite e di pari passo, all'interno di una cornice di politiche indirizzate ad incrementare il pari livello collettivo di sicurezza cyber, riducendo le dissomiglianze ed i divari in termini di disponibilità di risorse Lo sviluppo di una *digital health* nazionale dovrà quindi trovare piena realizzazione all'interno di un progetto di politiche pubbliche che sia organico e lungimirante di governance sanitaria, che promuova una condivisione selettiva dei dati sanitari, scongiurando la perdita di informazioni sensibili od il blocco dei sistemi interni, al fine di minimizzare i rischi cibernetici e le conseguenti possibili lesioni dirette alla sfera personale della riservatezza, della dignità e della safety degli individui.

CONCLUSIONI, NON CONCLUSIVE

Si voglia ivi ripetere il seguente concetto a fini riassuntivi: l'uso di Internet e delle ICT *(Information and Communications Technology)* costituisce, per il mondo sanitario, un meccanismo senza precedenti, propulsore di innovazione, atto a fornire risposte sempre più efficienti alle odierne problematiche legate alla salute. Maggiore informatizzazione e automazione dei processi tuttavia, se da un lato comportano nobili ed evidenti vantaggi, dall'altro, laddove non vengano sapientemente governati, rendono qualsivoglia struttura permeabile e terreno fertile per nuove forme di rischio.[344]

Tentando di pronosticare l'evolversi della sanità si può, a ben vedere, immaginare uno scenario futuro sempre più ibrido: alcune prestazioni sanitarie permarranno erogate "on site", ossia in presenza del paziente (negli ospedali, nelle strutture diagnostiche), altre rimarranno ibride, ossia in parte in presenza ed in parte virtuali (si pensi al telemonitoraggio ed alla telerefertazione), altre ancora diventeranno solo più virtuali (quali una televisita).

Il perimetro dunque da securizzare tenderà ad allargarsi, passando da una sanità "ospedalocentrica", ad un coinvolgimento domiciliare del cittadino, con un conseguente numero maggiore di dati in circolo e sempre più persone coinvolte nel, già complesso, organigramma sanitario.

Si voglia pertanto spostare l'attenzione sulle attuali sfide e sui conseguenti approcci che si pensa debbano essere adottati per farvi fronte.

Innanzitutto occorre assumere una piena consapevolezza circa l'ampiezza del tema, il problema della sicurezza infatti non è riconducibile solo al terreno puramente tecnologico, ma anzi va declinato sulla realtà aziendale nella sua interezza ed alla complessiva capacità di essere resiliente. Si riportino a questo proposito le parole di Schneier: *"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"*.[345] Peraltro ritenere che il CISO o il DPO siano le uniche figure a doversi

---

344 A. Antonilli, "Sicurezza informatica e trattamento dei dati in ambito sanitario", in *Salute e società,* XVI, suppl. 3/2017, pp. 97-98.

345 B. Schneier, *Schneier on security*, John Wiley & Sons, September 2008.

curare ed occupare delle tematiche inerenti alla sicurezza significa sviare la sua complessità, banalmente nel momento in cui si stipula un contratto di fornitura di beni o servizi occorrerà domandarsi se il fornitore, sebbene soggetto terzo, sia esso stesso in grado di fornire sicurezza. Da qui deriva l'attuale problema della *supply chain,* che non concerne quindi solamente i fornitori tecnologici (se si acquista Office 3.6.5 ci si può aspettare, a ben vedere, un certo livello di sicurezza garantito), ma anche coloro che, nonostante siano slegati da aspetti puramente informatici, devono parimenti essere responsabilizzati (si pensi ad un'azienda che distribuisce ossigeno ai pazienti terminali, questa avrà tutta una catena logistica di furgoni, mezzi ed operatori in grado accedere agli archivi di una azienda sanitaria e modificarne i dati contenuti, ad esempio laddove cambi il *caregiver* di un paziente). Si auspica quindi di far comprendere come tutta la catena plurisoggettiva dovrà essere responsabilizzata tramite procedure e protocolli sofisticati, anche se i soggetti protagonisti risultino prima facie estranei da quell'area puramente tecnologica maggiormente esposta al rischio.

Così Sergio Fumagalli, esperto CLUSIT:[346] *"Il tema da dover interfacciare è l'interoperabilità, andando cioè a toccare tutti i processi, le risorse umane ed ogni altra risorsa essenziale, che non sia soltanto IT, altrimenti si rimarrebbe bloccati in un'attitudine settoriale, come in una linea Maginot francese, invece il modello da adottare deve essere quello «svizzero», in cui tutte le persone di ogni cantone dedicano un mese all'anno per l'addestramento alla difesa del proprio cantone. Certo nella sanità il confine non si figura fisso e definito come quello svizzero, anzi si espande in continuazione, con nuovi cantoni (od unità) dando forma ad una realtà in cui addestrare e formare ciascuno per difendere il proprio tassello"*.

È così che si arriva nuovamente a ribadire il problema della formazione: a nulla servirà infatti dotarsi di sofisticati sistemi di *identity management* se poi l'operatore finale sanitario finisce per attaccare con un post-it sul proprio pc la password per accedere sistema. Una attuale sfida risulta allora far crescere una sempre maggiore cyber-cultura tramite corsi di aggiornamento e di formazione che appaiano

346 S. Fumagalli (intervento), al talk "Cybersecutity per la sanità digitale: conoscere per non rischiare", andato in onda il 28 Ottobre 2021, nella prima giornata di FORUM PA Sanità, evento digitale organizzato da FPA e P4I-Partners4Innovation.

stimolanti per gli operatori e che non vengano viceversa percepiti quali gravose lungaggini o perdite di tempo, da dover sostenere solo perché vi si è costretti.

Come fare concretamente?

Si ipotizzi la possibilità di programmare incontri diretti (invece che *online*) ravvicinati e collegiali, in presenza di tutti coloro che si ritrovano *day by day* ad operare sui dati, oppure si consideri la creazione di siti web e piattaforme FAQ (ossia, di *Frequently Asked Questions*) facilmente intuibili e dotati di rapide risposte, pare verosimile infatti ritenere che il personale sanitario voglia seguire procedure sicure, che spesso e volentieri però non sappia concretamente come fare. Peraltro non è più il tempo di mirare ad una formazione generale (e quindi, dispersiva), sarebbe invero preferibile cucirla ad hoc su ogni soggetto (primario, infermiere, fornitore etc.) di modo che concerna nello specifico i singoli tasselli operativi e gli obiettivi propri di ciascuno.

Questo è ad oggi il punto focale: la cyber-formazione deve essere sentita come obbligatoria, nonché avvertita come indispensabile per tutti, avvicinando l'offerta *know-how* con chi dovrà porre in essere determinati trattamenti, e nella sanità tutto ciò risulta difficile perché le priorità avvertite sono altre (quali la cura e l'assistenza puramente clinica dei pazienti). Com'è evidente, sarebbe più facile dotarsi di consulenti e di una svariata serie di procedure per ottemperare alla *compliance* richiesta piuttosto che "calarsi in basso", andando a toccare e correggere automatismi, nonché consuetudini di lavoro profondamente radicate che nessuno ha veramente l'intenzione di cambiare.

Resta il fatto che procedure tecnico-organizzative, set documentali, oneri burocratici e compliance non bastino più, occorre sopportare il costo (oneroso) del modificare alla radice il modo attuale di operare, perché il rischio di non farlo è, come si è visto, seriamente alto e cresce in misura esponenziale col crescere della pervasività della tecnologia. È evidente, ma pare comunque doveroso sottolineare che la sanità, quale sistema informativo complesso, necessiti di una attenzione costante nel tempo e di un approccio sistematico alle tematiche di sicurezza e privacy, che non sia viceversa sporadico, non servirà "correre dietro all'emergenza", anzi oggi più che mai vi è la forte necessità di stanziare budget pluriennali e

fissi da investire miratamente sulle tematiche inerenti alla sicurezza cyber.

Al fine di concretizzare quanto finora descritto il settore sanitario dovrà ad ogni modo rivedere e superare la sua attuale infrastruttura informatica, spesso eterogena e frammentata, facendo ricorso ad un approccio olistico che dia forma ad una governance in grado di coniugare sia misure di natura tecnica, sia aspetti organizzativi, procedurali, normativi ed in particolar modo di gestione ed analisi del rischio. A proposito di rischi, dal momento che ad oggi risultano tutti strettamente connessi, ed analizzabili di conseguenza in un'unica sintesi, allora tutti dovranno comparire dinnanzi alla Direzione strategica misurati e comparati, così da poter operare una valutazione obiettiva circa le esigenze da soddisfare, individuando dove investire sulla base dei punti di forza e debolezza individuati all'interno delle stesse Aziende sanitarie.

Da qui discende l'attuale urgenza di implementare e rafforzare il ruolo del *risk manager,* quale figura altamente multidisciplinare, in grado di abbracciare, comprendere e ponderare tutti gli ambiti del rischio. D'altra parte conseguire le competenze professionali necessarie a rivestire tale posizione è un processo, o meglio una evoluzione, in cui piuttosto che il curriculum formativo di partenza conta la formazione continua ed altresì l'aggiornamento costante lungo tutta la propria vita lavorativa circa ogni aspetto organizzativo, tecnologico, normativo o clinico che possa riguardare il rischio.

Questo è ciò che pare emergere: il reale bisogno di un *risk manager* che entri nei processi, che sappia ampliare le proprie competenze anche all'area della *business continuity* e alla gestione delle emergenze, una figura autorevole con una padronanza della materia, in grado di gestire la crescente complessità del nostro quotidiano. Tale esigenza si origina direttamente da alcune criticità e vulnerabilità che caratterizzano l'ambiente sanitario, prima fra tutti la scarsa conoscenza dei rischi, per come celati anche nelle operazioni più banali poste in essere da parte dei tanti operatori che si servono quotidianamente di *digital data e device,* inconsci spesso di cosa mettono in moto e della esposizione che possono provocare. Ancora, si osservi come il personale addetto alla sicurezza informatica risulti alle volte insufficiente, così come i ruoli legati propriamente al rischio cyber non sufficientemente definiti all'interno dello stesso organigramma sanitario,

la gestione dei sistemi tecnologici quindi pare abbisognare di maggiori addetti e nuovi ruoli professionali atti ad informare e dialogare periodicamente con gli stessi *risk manager*.[347] Pertanto, l'ambito dove risiede una maggior possibilità di miglioramento e, parallelamente, in cui vi è l'urgenza di adottare azioni e misure correttive, risulta essere la competenza, la formazione costante, ed anche la chiarezza dei ruoli, risultando l'investimento più promettente al fine di rafforzare ed implementare la resilienza e sicurezza informatica della sanità italiana.

Nel futuro prossimo l'unità organizzativa di *risk management* allora dovrà integrare nuove competenze e sperimentare nuovi modelli, che siano applicabili anche su scala nazionale, che prevedano il legame diretto tra *risk management* e Dirigenza strategica, riconoscendo allo stesso *risk manager* la possibilità di analizzare tutte le informazioni circa i vari rischi provenienti dai dipartimenti specialistici e determinare di conseguenza il livello di urgenza degli interventi di mitigazione. Se le organizzazioni sanitarie viceversa continueranno ad ignorare, o quantomeno sottostimare, l'importanza strategica del *risk management* sarà inevitabile assistere ad un forte e costante incremento dei cyber attacchi e delle conseguenze dannose in termini tanto di *privacy*, quanto di *safety e security*.

NOTE FINALI

Il presente elaborato tesistico rappresenta l'esito del percorso di ricerca svolto dall'autrice presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trento, sotto la supervisione del Professor Andrea Di Nicola, e discusso con lode il 15 marzo 2023. Successivamente, il lavoro è risultato vincitore della sesta edizione del premio "Una tesi per la sicurezza nazionale", assegnato il 10 dicembre 2024, iniziativa promossa dal Dipartimento delle Informazioni per la Sicurezza (DIS), con l'obiettivo di avvicinare le giovani generazioni al mondo dell'Intelligence, promuovendo e incentivando studi su tematiche legate alla sicurezza nazionale.

---

347 E. Sorano, A. Guerrieri, A. Sardi, "Criticità e consapevolezze" in *Capire il rischio cyber: il nuovo orizzonte in sanità,* whitepaper SHAM ITALIA, 2021, p. 42.

RIFERIMENTI BIBLIOGRAFICI

ABBOTT, *Important Cybersecurity Advisory: information about Cybersecurity Firmware Update,* Abbott Society, 28 August 2017.

ALBAMONTE E., "Il reato informatico nella prassi giudiziaria: le linee guida internazionali per il contrasto ai nuovi fenomeni criminali", in *Rivista Elettronica di Diritto, Economia, Management*, n. 3, 2013, p. 146-157.

ALCATEL L. ENTERPRISE, *Sicurezza informatica della rete sanitaria nell'era della trasformazione digitale: con una intervista a Silvia Piai, Research Director per IDC Health Insights,* ALE international, 2020.

AMATO G., "I reati informatici e le modifiche apportate dalla legge n. 48/2008", in G. Amato, V. Desposito, G. Dezzani, C. Santoriello (a cura di), *I reati informatici,* CEDAM, Mlano, 2010, pp. 27-122.

AMATO G., SANDRO DESTITO V., DEZZANI G., SANTORIELLO C., I *reati informatic*i, CEDAM, La biblioteca del penalista, Milano, 2010.

ANANDRAO S. S., "Virus approach", in *International Journal of Network Security and Its Applications* (IJNSA), Vol. 3, N. 4, July 2011, pp. 33-46.

ANITEC-ASSINFORM, *Una data strategy per la Sanità italiana,* a cura del gruppo di lavoro Digital Transformation in Sanità di Anitec-Assinform, Maggio 2022.

ANTONILLI A., "Sicurezza informatica e trattamento dei dati in ambito sanitario", in Salute e società, XVI, suppl. 3/2017, pp. 84-100.

APRUZZESE A., "Autori e vittime nella criminalità informatica", *in Rivista di Criminologia, Vittimologia e Sicurezza,* Vol. III, n. 3 - Vol. IV, n. 1, Settembre 2009 - Aprile 2010, pp. 101-106.

ASPR, *Healthcare system cybersecurity: Readiness & Response Considerations,* ASPR (Administration for strategic preparedness and response) – TRACIE (healthcare emergency preparedness information gateway), originally published February 2021, Updated October 2022.

APRUZZESE A., "Dal computer crime al computer-related crime", in *Rivista di Criminologia, Vittimologia e Sicurezza,* Vol. I, n.1, Gennaio 2007 pp. 1-6.

ATERNO S., CAIANI F., COSTABILE G., CURTOTTI D., *Cyber forensics e indagini digitali: manuale tecnico giuridico e casi pratici,* Giappichelli Editore, Torino, Aprile 2021.

BALBONI P., TUGNOLI F., "Reati informatici e tutela dei dati personali: profili di responsabilità degli enti", in *Giurisprudenza Penale,* 2021/1-bis , pp. 3-8.

BARNES S.B., "A privacy paradox: Social networking in the United States", *in First Monday,* Issue 11/9, 2006.

BARTOLI L., MAIOLI C., "La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti", in *Informatica e diritto,* XLI annata, Vol. XXIV, n. 1-2, 2015, pp.139-151.

BERTINI U., *Introduzione allo studio dei rischi nell'economia aziendale,* Giuffrè Editore, Milano, 1987.

BHUYAN S., KABIR U., ESCARENO J. M. ECTOR K., PALAKODETI S., WYANT D. et al., "Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations", in *Journal of Medical Systems,* Vol. 44/98, 2 April 2020.

BOLOGNINI L. (intervento), Presidente dell'Istituto italiano per la privacy, avvocato ICT Legal Consulting, al Convegno Privacy Unolegal, Milano, 14 Giugno 2017.

BOLOGNINI L., PELINO E., *Codice privacy: tutte le novità* del D.lgs. 101/2018, Giuffrè Editore, Milano, 2019.

BONACI T., *To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robotics,* Department of Engineering, University of Washington, 2015.

BONFANTI M. (intervista), Convegno "Cybersecurity e protezione dei dati personali nella sanità: un nodo strategico per l'interesse nazionale", Fondazione ICSA in partnership con Link Campus University, 16 Giugno 2022.

BORRUSO R., "La tutela del documento e dei dati", in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), *Profili penali dell'informatica,* Giuffrè Editore, Milano, 1994, p. 29 ss.

BRAR H., KUMAR G., "Cybercrimes: a proposed taxonomy and challenges", in *Journal of computer networks and communication,* 2018.

BRENNER S., "Defining cybercrime: a review of state and federal Law", in R.D. Clifford, *Cybercrime: The investigation, prosecution of a computer-related crime,* Carolina Academic Press, Durham, 2006, pp. 15-104.

BREWSTER B., KEMP B., GALEHBAKHTARI S., AKHGAR B., "Cybercrime: attack motivations and implications for big data and national security", in Staniforth A., Akhgar B., Saathoff G .B., Hill R., Arabnia H. (a cura di), *Application of big data for national security. A practitioner's guide to emerging technologies,* Elsevier, Amsterdam, 2015, pp. 108-127.

BRISCHETTO R., COSMI F., *Imparare il metodo scientifico. Da Ippocrate a Garattini,* Edizioni LSWR, Milano, 2022.

BRZEZINSKI D., KILLALEA T., *"Guidelines for evidence collection and archiving",* The Internet Society, February 2002.

BUTTER M., RENSMA A., et al., *Robotics for ealthcare: Final report, European* Commission, DG information society, 3 Ottobre 2008.

BUTTI G., PIAMONTE A., *GDPR: nuova privacy. La conformità su misura,* Iter editore, Milano, 2017.

CARLINO F., "Il trattamento dei dati sanitari mediante il dossier sanitario", in *Iusinitinere*, Rivista Semestrale di diritto, ISSN 2724-2862, 29 Maggio 2020, pp. 1-3.

CARLINO F., "L'origine della privacy e l'esigenza di tutelare i dati personali", in *Iusinitinere*, Rivista Semestrale di diritto, ISSN 2724-2862, 4 Luglio 2020, aggiornato 13 Luglio 2020, pp. 1-13.

CASTELLS M., *La nascita della società in rete,* Egea, Milano, 2022.

CECCACCI G., *Computer Crimes: la nuova disciplina dei reati informatici,* FAG, Milano, 1994.

CHIARINI G., "Privacy: come cambia il dato normativo", in *E-Health: innovazione e tecnologia in ospedale,* vol. 72, 2019, p. 66-69.

CLOUGH J., "A world of Difference: The Budapest Convention on Cybercrime and the challenges of Harmonization", in *Monash University Law Review*, Vol. 40, n. 3, 2014.

CLUSIT, *Rapporto Clusit sulla sicurezza ICT in Italia,* report Edizioni 2020 – 2022.

CINI - Cybersecurity National Lab, *Il futuro della Cybersecurity in Italia: ambiti progettuali strategici, progetti ed azioni per difendere al meglio il Paese dagli attacchi informatici,* Laboratorio Nazionale di Cybersecurity - CINI Consorzio interuniversitario Nazionale per l'Informatica, 9 Ottobre 2018.

CIPOLLA C., ARDISSONE A., "Un paradigma cittadino-centrico nella m-Health", in *Salute e società,* XVI, n. 2, 2017, p.12-28.

COLOMBO E., La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali", in *Ciberspazio e diritto: Internet e le professioni giuridiche,* Vol. 10, n. 3/4, 2009, pp. 285-304.

CORCELLA R., "Attacchi informatici in aumento nel settore sanitario", in *Corriere Salute,* Raffaello Cortina Editore, 10 Marzo 2022, p. 16.

CORRADINI I., "Il crimine informatico in azienda", in G. Marotta (a cura di), *Tecnologie dell'informazione e comportamenti devianti,* Edizioni Universitarie di Lettere Economia Diritto, Milano, 2004.

CORTESI A., "L'art. 25 del GDPR: dalla privacy by default al principio di minimizzazione o necessità nel trattamento dei dati personali", in *Interlex: rivista di diritto, tecnologia, informazione,* pubblicazione iscritta nel registro della stampa del Tribunale di Roma con il n. 585/97, 2017.

COVENTRY L., BRANLEY D., "Cybersecurity in healthcare: a narrative review of trends, threats and ways forward, in *National Library of Medicine,* 22 July 2018, pp. 48-52

CREST, *Cyber Security Incident Response Supplier Selection Guide,* Version 1, 2013.

CUOMO L., RAZZANTE R., *La nuova disciplina dei reati informatici,* Giappichelli, Torino, 1 Maggio 2009.

CYNERIO, *The State of Healthcare IoT Device Security* 2022, Cynerio, 2022.

D'ACQUISTO G., NALDI M., *Big Data e Privacy by Design. Anonimizzazione, Pseudonimizzazione* e Sicurezza, Giappichelli Editore, Torino, 2017.

D'ALESSANDRO L., "Prefazione", in A. Pitasi (a cura di), *Webcrimes. Normalità, devianze e reati nel cyberspace*, Guerini e Associati, Milano, 2007.

DE LUCA V., DI SANT'AGATA G. M., VOCE F., *Il ruolo dell'Italia nella sicurezza cibernetica: minacce, sfide e opportunità,* FrancoAngeli, Milano, 2018.

DE LUCIA, "L'analisi tecnica: LockBit, chi è e come agisce la gang del ransomware", in *Cybersecurity360,* testata editoriale di Digital360, 12 Agosto 2021.

DEL GAUDIO F., "La sicurezza dei dispositivi medici ospedalieri connessi a rischio hacker", in *Filodiritto: quotidiano di diritto, cultura e società , 3 Maggio 2022.*

DI CIOMMO F., "Il trattamento dei dati sanitari tra interessi individuali e collettivi", in R. Pardolesi (a cura di), *La privacy sanitaria,* vol. II, Giuffrè editore, Milano, 2003.

DI GERONIMO F., MAGGIA C., "La gestione dei ransomware, un approccio multidisciplinare", in *Privacy& Data Protection, Technology, Cybersecurity,* n. 1, Aprile 2022, Egea, pp. 74-99.

DI FEDE, I. CORRADINI, "Hacker e internet crime", in G. Marotta (a cura di), *Tecnologie dell'informazione e comportamenti devianti,* Edizioni Universitarie di Lettere Economia Diritto, Milano, 2004.

DI NICOLA A., *Criminalità e criminologia nella società digitale*, FrancoAngeli, Milano, 2021.

DISTEFANO N., "Risk Management e Metodi di Risk Assessment: Tecniche per la valutazione del rischio", presentazione presso DICAR (Dipartimento di Ingegneria Civile e Architettura), in data 2 Luglio 2020.

DLA PIPER Studio Legale, "Cybersecurity nell'uso dei dispositivi medici: nuova guida del Medical Device Coordination Group", in *Diritto al Digitale,* 21 Gennaio 2020.

DOMENICALI C., "Tutela della persona negli spazi virtuali", in *Federalismi.it Rivista di diritto pubblico italiano, comparato, europeo,* ISSN 1826-3534, n. 7, 28 Marzo 2018, pp. 10-14.

DONATI L., VACIAGO G., "Compliance 231: Modelli organizzativi e OdV tra prassi applicative ed esperienze di settore", Gruppo Sole 24 Ore, Milano, 2022.

DONINI M., *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà,* in A. Bernardi, M. Donini, V. Militello, M. Pasa, S. Seminara (a cura di), Collana quaderni di diritto penale comparato, Internazionale ed Europeo, Milano, Giuffrè editore, 2004.

DUCCI G., *Pianificare la comunicazione dei servizi di e-health*: *attori, sistemi, relazioni. Il caso del fascicolo sanitario elettronico,* in Sociologia della comunicazione, fascicolo 48, 2014, pp. 26-37.

ECRI INSITUTE, "Top 10 Health technology Hazards for 2015", in *Health Devices,* November 2014, pp. 26-29.

ENISA, *Procurement guidelines for cybersecurity in hospitals: good practices for the security of Healthcare services,* European Union Agency for Cybersecurity, Athens Office, February 2020.

ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches,* European Union Agency for Network and Information Security (ENISA), Working document V. 10, December 2013.

ENISA, *Un Europa affidabile e sicura dal punto di vista informatico: La strategia Enisa,* Agenzia dell'Unione europea per la cibersicurezza, Atene, Giugno 2020.

EUROBOTICS AISBL, (Association Internationale Sans But Lucratif), *Strategic agenda for Robotics in Europe* 2014-2020, 11 Ottobre 2013.

EXPRIVIA, "Maze e ransomware as a service: sanità sotto minaccia della doppia e tripla estorsione", in *Cybersecurity360*, 22 Giugno 2021, pp. 2-5.

EYSEBENCH G., "What is e-Health, in Journal of Medical Internet Research", in *Journal of Medical Internet Research,* 3(2), 2001, p. 20.

FARRINGER D., "Maybe if we turn it off and then turn it back on again? Exploring Health Care Reform as a means to curb cyber-attacks", in *Journal of Law, Medicine & Ethics,* 47(S4), 2019, pp. 91-201.

FATTAH E.A., "Victimology: past, present and future", in *Criminologie,* 33(1), 2020 pp. 17-46.

FBI, *Indicators of Compromise associated with LockBit 2.0*, FBI Cyber division, 4 February 2022.

FINOCCHIARO G., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli editore, Bologna, 2017.

FIORIGLIO G. "La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici", in *Journal of Ethics and Legal Technologies*, Volume 3(2), Novembre 2021, pp. 85-86.

FLOR R., FALCINELLI D., MARCOLINI S., *La giustizia penale nella "rete": le nuove sfide della società dell'informazione nell'epoca di Internet,* Edizioni DiPlaP, Milano, 2015.

FORNARI G., *Il trattamento dei dati: rischi penali e compliance dell'impresa,* Fornari e Associati studio legale, Milano-Roma, Gennaio 2021.

FORTIN F., *Cybercriminalité Entre inconduite et crime organisé,* Presses internationales Polytechnique et Sûreté du Québec, Canada, 2013.

FRANZO M., D'AGOSTINO F., et al. "Does a medical device nomenclature suitable for all purposes exist? Twenty years of Italian experience with the CND and its adoption in EUDAMED at European level", in *European Medical Device Nomenclature implementation working group project,* Trieste, June 10th-12th, 2020.

FRASER B., *RFC2196 : Site Security Handbook,* RFC Editor, USA, 1997.

FROSINI V., *Contributi ad un diritto dell'informazione,* Liguori, Napoli, 1991.

FUMAGALLI S. (intervento), al talk "Cybersecutity per la sanità digitale: conoscere per non rischiare", il 28 Ottobre 2021, nella prima giornata di FORUM PA Sanità, evento digitale organizzato da FPA e P4I-Partners4Innovation.

GALDIERI P., "Il reato informatico", in G. Marotta (a cura di), *Tecnologie dell'informazione e comportamenti devianti,* Edizioni Universitarie di Lettere Economia Diritto, Milano, 2004 , pp. 29-74.

GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico,* Giuffrè editore, Milano, 1997.

GALLINO L., *Dizionario di sociologia,* Utet, Torino, 2006.

GALLOTTI C., *Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma* IOS/IEC 27001, Lulu Press Inc., Raleigh, 28 Gennaio 2019.

GELPI A., "La Sicurezza dei dati sanitari", in *Torino Medica. La rivista dell'ordine dei medici chirurghi e odontoiatri della provincia di Torino*, anno XXXIII, numero 3-4, 2021, pp. 11-21.

GHAFUR S., GRASS E., JEGGINGS N. R., "The challenges of cybersecurity in health care: the UK National Health service as a case study", in Lancet Digit Health, Volume 1, issue 1, May 2019, pp. 10-12.

GHIGLIA A. (intervista), componente del Garante per la protezione dei dati personali, "La sanità la più colpita. Proteggere reti e dati sensibili", di Luigi Garofalo, 9 Novembre 2021.

GHIRARDINI A, FAGGIOLI G., Computer Forensics, Apogeo Editore, Milano, 2009.

GIBSON W., *Neuromante*, Mondadori, Milano, 2003.

GRIFFIN N., Health correspondent, "Patient data 10-15 times more valuable than credit card data", in *Irish Examiner,* 19 Maggio 2021.

IEZZI P. (intervista), pubblicata il 14.05.2022, ad opera di Massimo Canorro, sul Quotidiano Sanitario Nazionale Nurse24.

INDIPENDENT SECURITY EVALUATORS, *Securing Hospitals: a research study and blueprint,* 23 February 2016.

JAISHANKAR K., "Cyber victimology: a new sub-discipline of the twenty-first cen-

tury victimology", in J. Joseph, S. Jergenson (a cura di) *An international perspective on contemporary developments in victimology,* Springer, Cham, 2020, pp. 3-19.

JALALI M. S., KAISER J. P., "Cybersecurity in hospitals: a systematic, organizational perspective", in *Journal of medical Internet Research,* Vol. 20, iss. 5, 2018, pp. 1- 16.

KASPERSKY, EDR & MDR: *tutto ciò che occorre sapere: definizioni, funzionalità e vantaggi,* Kaspersky Lab., 2021.

KASPERSKY, *Telehealth take-up: the risks and opportunities,* healthcare report 2021.

KESSLER G. C., Are mobile device examinations practiced like Forensic?", in *Digital Evidence and Electronic Signature,* Vol. 12, 2015.

KRUSE W. G., HESIER J.G., *Computer Foresnsics*, *Incident Response Essentials,* Addison-Wesley, 2002.

KUEHN B. M., "Pacemaker recall highlights security concerns for implantable devices", in *Circulation-Cardiology* News, n. 138, 9 October 2018, pp. 1597-1598.

LAGIOIA, F., *L'intelligenza artificiale in sanità: un'analisi giuridica,* Giappichelli Editore, Torino, 2020.

LEVITA L., , "La disciplina sostanziale: i reati informatici in senso stretto", in G. D'aiuto (a cura di) *I reati informatici: disciplina sostanziale e questioni processuali,* Giuffrè Editore, 2012, pp. 3-91.

LEVY, *Hacker, gli eroi della rivoluzione informatica,* Shake Editore, Milano, 1996.

LIMONE E., "Sanità digitale: scenari scatenati da un data breach", in *Agendadigitale.eu*, Editore ICT&Strategy, Gruppo Digital360, Milano, 1 Luglio 2019.

LOCATELLI P., ZACCHETTI D., FERRARA F., "I modelli necessari a strutturare un clinical data repository", in *Progettare per la sanità*, n. 5, Ottobre 2019.

LORUSSO P., *L'insicurezza dell'era digitale: tra cybercrimes e nuove frontiere dell'investigazione,* FrancoAngeli, Milano, 2011.

LUGARESI N., *Internet, privacy e i pubblici poteri negli Stati Uniti*, Giuffrè editore, Milano, 2000.

MACILOTTI G. , "La criminalità informatica e telematica fra antichi dilemmi e nuove sfide", in A. Balloni, R. Bisi, R. Sette (a cura di), *Principi di criminologia applicata. Criminalità, controllo, sicurezza,* Wolters Kluwer-Cedam, Milano, pp. 251-277.

MACILOTTI G., "Studiare la cybercriminalità: alcune riflessioni metodologiche", in *Rivista di criminologia, vittimologia e sicurezza,* Vol. XII, N. 1, 2018, pp.52-80.

MACRÌ E., "Il quadro giuridico del cyber risk", in *Capire il rischio cyber: il nuovo orizzonte in sanità, whitepaper* SHAM Italia, 2021, pp.15-22

MANDRIOLI D., "Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli stati", in *La comunità scientifica,* Fasc. 3/2018, Editoriale scientifica Srl, pp. 473-492.

MANTOVANI F., *Diritto penale. Parte Speciale:* I, CEDAM, Torino, 2014.

MANZI E., SELVAGGI S., SICA V., "Tecnologie informatiche e delle comunicazioni in medicina: la telemedicina", in V. Sica, S. Selvaggi (a cura di), L*a telemedicina. Approccio multidisciplinare alla gestione dei dati sanitari,* Springer-Verlag, Milano, 2010, pp. 1-9.

MARESCAUX J., LEROY J. et al., "Transatlantic robot-assisted telesurgery", in *Nature*, vol. CDXIII, n. 6854, September 2001, pp. 379-380.

MARION N. E., "The Council of Europe's Cyber Crime Treaty: An exercise in symbolic legislation", in *International Journal of Cyber Criminology*, Vol. 4, n. 1-2, 2010, pp. 699-700.

MAROTTA G., T*ecnologie dell'informazione e comportamenti devianti*, Edizioni Universitarie di Lettere Economia Diritto, Milano, 2004.

MARTIN G., MARTIN P., HANKIN C., DDARZI A., KINROSS J., "Cybersecurity and healthcare, how safe are we?", in *BMJ*, 06 July 2017.

MASON S., *Electronic Evidence: disclosure, discovery, and admission*, LexisNexis Butterwoorths, London, 2007.

MASON S., *International Electronic Evidence*, British Institute of International and Comparative Law, London, 2008.

MCELROY R., KELLERMANN T. *Healthcare Cyber Heists in 2019: 20 leading CISOs from the healthcare industry offer their perspective on evolving cyberattacks, ransomware & the biggest concerns to their organizations,* Carbon Black, June 2019.

MCGUIRE M., DOWLING S., *Cybercrime a review of the evidence. Research report 75, Home Office*, Londra, 2013.

ME G., "La sicurezza dei sistemi informatici aziendali", in T*ecnologie dell'informazione e comportamento devianti*, Milano, 2004, pp. 101-135.

MEDTRONIC, *Urgent Field Safety Notice: MiniMed remote controller (MMT-500 or MMT-503),* August 2018; *Urgent Medical Device Recall: MiniMed remote controller (MMT-500 or MMT-503),* October 2021.

MEGGITT, "Medjack attacks: the scariest part of the Hospital", in *Tufts University Press,* December 12th 2018.

MELAND P. H., BAYOUMY Y.F., SINDRE G., "The ransomware-as-a-Service economy within the darknet" in *Computers and Security,* Vol. 92, 29 February 2020, pp.1-8.

MINISTRY OF HEALTH (Singapore), *Healthcare Cybersecurity Essentials*, CSA (Security Agency of Singapore), August 2021.

MITNICK K. *L'arte dell'inganno,* Feltrinelli, Milano, 2013.

MONTEROSSI M. W., "Responsabilità civile e cybersicurezza nell'ecosistema dell'Internet delle cose", in *Giustiziacivile*, 2020, pp. 1-46.

MONTESSORO P., "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Istituzioni del federalismo*, n.3, 2019, pp. 783-800.

MORUZZI M., "La nuova cultura della sanità dematerializzata", in *Recenti Progressi in Medicina*, vol. 105, n.11, 2014, p. 407- 409.

MUKARSEY M., SEDWICK J., HAGY D., *Electronic crime scene investigation: a guide for first responders, Second Edition*, U.S Department of Justice Special Report, April 2008.

NETPATROL, "Sanità digitale e telemedicina: privacy, cybersicurezza e intelligenza artificiale nella sanità digitale", in *GDPR insight series*, n° 6, 2020, pp. 2-16.

OSTERMAN RESEARCH, *Cyber security in Healthcare,* Whitepaper, February 2020.

PEJČINOVIĆ B. M. (intervento), Conferenza ed apertura alla firma del Secondo Protocollo addizionale alla Convenzione sulla criminalità informatica, 12 Maggio 2022.

PERRI P. (intervento), durante il Webinar "Conoscere e prevenire gli attacchi cyber in sanità", tenutosi in data 30 giugno 2021.

PICA G., *Teoria e pratica nell'interpretazione del reato informatico,* Giuffrè editore, Milano, 1997.

PICA. G. *Diritto penale delle tecnologie informatiche,* UTET, Torino, 1999.

PIERATTONI D., "La direttiva NIS2: nuovi obblighi e opportunità", in Sicurezza e Giustizia, V. II, MMXXII, pp. 34-37

PIERGALLINI C., , "I delitti contro la riservatezza informatica" C. Piergallini, F. Viganò, M. Vizzardi, A. Verri (a cura di) in *Delitti Contro la persona,* CEDAM, Padova, 2015.

PIETRELLA T., "Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle Botnets", in *Discrimen - Rivista di diritto penale,* ISSN 2704-6338, 2.12.2021, pp. 2-7.

PINTUS E., *Scelte pubbliche e strumenti di management per gli acquisti*, McGraw-Hill, Milano, 2009.

POLETTI D., "Comprendere il Reg. UE 2016/679: Un'introduzione", in A. Mantelero, D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna,* Pisa University Press, 2018, pp. 9-19.

POMANTE G., *Hacker e computer crimes,* Volume 41/15, Edizioni Simone, Napoli, 2000.

PONEMON INSTITUTE, *Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care, independently* conducted by Ponemon Institute, 2022.

PONTI G., *Compendio di criminologia,* Cortina, Torino, 1994.

PRESS RELEASE, "Security Union: Commission welcomes today's political agreement on new rules to enhance the resilience of critical entities", in occasione dell'accordo raggiunto fra il Parlamento Europeo ed il Consiglio dell'Unione Europea circa l'approvazione della Direttiva CER, 28 June 2022, Bruxelles.

REEP-VAN DEN BERGH C.M.M., JUNGER M., "Crime science", in *Victims of cybercrime in Europe: a review of victim surveys,* 7(5), 2018, pp. 1-15.

RESCIGNO P., *Diritti della personalità,* Enciclopedia Giuridica Treccani, Roma, 1994.

RICCIO R., "Le misure di sicurezza tra GDPR e ISO 27001: due normative a confronto e i possibili scenari prospettabili", in *Cyberlaws: free legal database and blog,* 9 Gennaio 2019.

ROCCHI W., "Cyber security nel settore sanitario, a rischio apparecchiature mediche e dati riservati: lo scenario", in *Cybersecurity360,* testata editoriale di Digital360, 5 Maggio 2020.

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli,* Laterza-la Repubblica, Roma-Bari, 2014.

RODOTÀ, "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali", in *Rivista critica di diritto privato*, anno XV, 1997, pp. 583-609

SALTZER J., "The protection of Information in Computing System", in *Proceedings of the IEEE,* v. 63 n.9, 1975, pp. 1278-1308.

SALVADORI A., "Deontologia e tutela dei dati sanitari", in *Torino Medica. La rivista dell'ordine dei medici chirurghi e odontoiatri della provincia di Torino,* anno XXXIII, numero 3-4, 2021, pp. 9-10.

SANTORO E., PANSADORO V., *La chirurgia robotica in Italia : indagine nazionale,* 2011.

SARZANA C., *Informatica, internet e diritto penale,* Giuffrè Editore, Milano, 2010.

SASSI S., *Il sistema dei rischi d'impresa,* Vallardi Editore, Milano, 1940.

SAVINO C., "Cyber risk, assicurazioni e PMI", presentazione per *Ania*: Associazione Nazionale fra le imprese assicuratrici, 7 Marzo 2017.

SCHNEIER B., *Schneier on security,* John Wiley & Sons, September 2008.

SETOLA R., ASSENZA G., "Recepimento della direttiva NIS sulla cyber-security delle reti", in *Sicurezza e Giustizia*, n. IV, 2018, pp. 32-35.

SETOLA R. (intervista) dell'Università Campus Bio-Medico di Roma durante la seconda giornata del convegno "Big Data in Health", riportata in *Sanità Informazione,* da Franzellitti V., Cavalcanti G., 3 Ottobre 2019.

SHAM ITALIA, *Capire il rischio cyber: il nuovo orizzonte in sanità,* whitepaper SHAM Italia, 2021.

SMITH S., KOPPEL R., "Healthcare Information Technology's Relativity Problems: A Typology of How Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ", in *Journal of the American Medical Informatics Association,* 21, no. 1, January 2014, pp. 117–31.

SMORALDI L., STRAZZULLO M. "Prevenire è meglio che curare: il compito dell'avvocato in caso di data breach", in *Data Protection Law: diritto delle nuove tecnologie, privacy e protezione dati personali* - Rivista online Giuridica Semestrale, n. 2, 2021, p. 73.

SOLINAS M., "Tutela penale della privacy dopo il Gdpr: la frettolosa giustappo-

sizione delle fonti è scaturigine di un sistema farraginoso che crea confusione, in *Responsabilità Civile e Previdenza,* fasc. 2, Vol. 85, 1 Gennaio 2020, pp. 663-688.

SORANO E., GUERRIERI A., SARDI A., "Criticità e consapevolezze" in *Capire il rischio cyber: il nuovo orizzonte in sanità,* Whitepaper SHAM ITALIA, 2021.

SORO A. (intervento), "Big Data: La nuova geografia dei poteri", in occasione della Giornata Europea della protezione dei dati personali, 30 Gennaio 2017.

SORO A. (intervento), "La smaterializzazione dei documenti e il suo impatto sul sistema salute", Convegno tenutosi a Roma 6 Maggio 2016.

SORO A. (intervento), "Il Garante: un caso di straordinaria gravità", riportata sul Corriere della Sera - Ed. Bergamo, 31 Ottobre 2013, di G. Ubbiali.

SORO A. (intervento), "Tracciamento contagi coronavirus, ecco i criteri da seguire", in Agenda Digitale, 29 Marzo 2020.

SOURNIA J., *Storia della Medicina,* edizioni Dedalo S.r.l., Bari, 1994.

STANZIONE P. (intervento), "Sicurezza del dato sanitario e condivisione", in *Panorama*, 18 Febbraio 2022.

STEPHENSON P. GILBERT K., *Investigating Computer Related Crime: Second Edition,* CRC Press, Routledge, 5 June 2002.

STERLING B., *Giro di vite contro gli hacker* (The hacker crackdown), Shake Edizioni Underground, Milano, 1996.

STILO L., "Il danneggiamento informatico: genesi e aspetti problematici della fattispecie, in *Diritto & Diritti,* Rivista Giuridica online, Dicembre 2003.

STRANO M., *Computer Crime*, Apogeo Editore, Milano, 2000.

SULER J., "The Online Disinhibition Effect", in *Cyberpsychology & behavoir,* 7(3), pp. 321-326.

TELMONI C. (intervento), talk "Cybersecutity per la sanità digitale: conoscere per

non rischiare", andato in onda il 28 Ottobre 2021, nella prima giornata di FORUM PA Sanità, evento digitale organizzato da FPA e P4I-Partners4Innovation.

THE MENTOR (BLANKENSHIP L.), *The conscience of a Hacker*, e-zine Phrack, Volume 1, Issue 7, Phile 3, 8 January 1986.

TREND MICRO, *Defending the Expanding Attack Surface: Midyear Cybersecurity Report*, Trend Micro Research, global leader in Cybersecurity, 2022.

TREND MICRO, *Cybercrime and Other Threats Faced by the Healthcare Industry,* Mayra Rosario Fuentes Forward-Looking Threat Research (FTR) Team, 2017.

VULPIANI D., "La nuova criminalità informatica. Evoluzione del fenomeno", in *Rivista di Criminologia, Vittimologia* e Sicurezza, Vol. 1, n.1, Gennaio - Aprile 2007, pp.1-9.

WALL D. S., "Digital realism and the governance of spam as cybercrime", in *European journal on criminal policy and research,* 10(4), 2005.

WALL, DAVID S., *Crime and the internet*, Routledge, New York, 2001.

WARREN S., BRANDEIS L.D., "The right to Privacy", in *Harvard Law Review,* Vol. 4, No. 5, 1890, pp.193-220.

WARREN M., LEITCH S., "Hackers Taggers: A new type of hackers", in *School of Information Systems, Deakin University press,* Springer, 7 August 2009, pp. 425-431.

WASSERMAN L., WASSERMAN Y., "Hospital cybersecurity risks and gaps: Revie (for the non-cyber-professional)", in *Frontiers in Digital Health*, 11 August 2022, pp. 1-17.

WEBER A. M., "The Council of Europe's Convention on Cybercrime", in *Berkeley Technology Law Journal,* Vol. 18, n. 1, 2003.

WEULEN M. KRANENBARG, "Contrasting cyber-dependent and traditional offenders. A comparison on criminological explanations and potential prevention

methods", in E.R. Leukfeldt, T. Holt (a cura di), *The Human factor of cybercrime,* Routledge, Londra, 2020, pp. 194-215.

WHEELER D. A., *Secure Programming HOWTO*, v 3.72 Edition, 2015.

ZAGARIA C., *L'enterprise Risk Management: gestione del rischio, profili di comunicazione ed evidenze empiriche*, Giappichelli Editore, Torino, 2017.

ZSCALER, *Le tre chiavi per la trasformazione attraverso l'approccio zero trust: piattaforma, persone e processo*, Zscaler Inc., 2021

6 - 7 maggio 2026

AUDITORIUM DELLA TECNICA, ROMA

CYBER CRIME CONFERENCE

14ª EDIZIONE

ICTSECURITYMAGAZINE.COM