DOCUMENTO DI SINTESI

Alessandro Colucci, Presidente I Commissione, Programmazione Bilancio Regione Lombardia – ha portato i suoi saluti istituzionali e ha parlato del tema della sicurezza dei dati, a partire da quelli sanitari, il lavoro di Regione Lombardia è partito da tempo in un contesto nazionale ben lontano dall'aver preso consapevolezza dell'importanza di questo argomento. Per questo è necessario partire dalla diffusione di questa cultura a tutti i livelli della nostra società, dalle imprese agli enti pubblici ai singoli cittadini. Sarà quindi indispensabile la preparazione e diffusione di figure professionali esperte del tema, che possano discriminare le tipologie dei problemi e scegliere le soluzioni più opportune, anche attraverso un'azione preventiva. Come Regione abbiamo già avviato in Lombardia un Tavolo di confronto con tutti gli stakeholder, che ha già prodotto un primo, proficuo confronto nella convention del 6 aprile scorso a Palazzo Lombardia, in occasione dell'insediamento della "Cabina di regia" sulle politiche di ricerca e innovazione.

Angelo Capelli, Vicepresidente III Commissione, Sanità e politiche sociali Regione Lombardia I sistemi che non si adattano sono sistemi che da un punto di vista finanziario sono destinati a saltare. Il futuro del dato nel campo della salute pubblica è il cloud. I vantaggi sono almeno due: prima di tutto l'immagazzinamento delle informazioni consente una fruizione più agile delle informazioni tra i vari operatori sanitari. In secondo luogo, con l'acquisizione dei dati è possibile fare alcune predizioni in merito a determinate patologie e gestire al meglio i nuovi test clinici partendo da campioni molto più ampi. È bene, però, preoccuparsi di gestire le modalità e gli strumenti che mettano in sicurezza questi dati e devono essere anche ben organizzati con un adeguato supporto informatico e individuando settori di intervento mirati. Questo, chiaramente, si ripercuote positivamente sui costi.

Gabriele Faggioli, Presidente Clusit – Il tema della sicurezza informatica è all'ordine del giorno di tutte le strutture sanitarie pubbliche e private. I recenti casi di cronaca dimostrano che la sanità è un settore che i criminali informatici aggrediscono frequentemente come peraltro

dimostrato dai dati raccolti dal Clusit. Lo scenario è complesso e le misure da adottare devono essere varie ma non si può impostare una strategia difensiva efficace solo su un piano tecnologico. Occorre maggiore cultura dei rischi a cui siamo sottoposti e comprensione della complessità e delle possibili minacce che discendono dall'uso delle tecnologie.

Stefano Quintarelli, Presidente del Comitato di Indirizzo dell'Agenzia per l'Italia digitale - Lo scenario tecnologico cambia molto velocemente ed è in questo contesto di cambiamento che si vanno ridefinendo le filiere: con l'Industria 4.0 cambia il rapporto azienda-clienti. Quintarelli ha poi spiegato la questione "sicurezza", un tema non solo tecnologico ma anche culturale. Nei prossimi anni ogni oggetto sarà collegato all'altro, ci saranno computer ovunque, cambieranno scenari e processi nel mondo del lavoro, perciò la security è un tema delicato da affrontare. Tuttavia, non ha senso opporsi all'evoluzione hi-tech. Istruzione, formazione e welfare faranno la differenza. Essa richiede una maggiore consapevolezza che questa nuova dimensione è legata indissolubilmente all'infosfera digitale in cui ciascuno è immesso. Forse nel breve periodo sarà difficile accrescere la "consapevolezza digitale" dei parlamentari, ma si può essere più ottimisti nel medio e lungo termine, perché l'economia si trasforma. Senza la trasformazione digitale l'economia si ferma, facendo mancare anche le risorse pubbliche, già oggi scarse. Questo spostamento del valore aggiunto verso il digitale rende necessaria una maggiore consapevolezza anche tra i parlamentari, forse già a partire dalla prossima legislatura.

Alessandra Poggiani, Direttore Generale di Venis, Venezia Informatica e Sistemi - L'Italia è tra i paesi in Europa che ha un maggior numero di servizi digitali offerti dalla pubblica amministrazione, ma con un basso tasso di utilizzo dei servizi, coerente con un basso livello di alfabetizzazione digitale dei cittadini. È un paese caratterizzato da un satellite, che gravita attorno alle grandi città, costituito da piccole realtà territoriale dove ancora il rapporto personale di sportello è forte. I servizi digitali non sono disegnati sulla modalità secondo cui i cittadini cercano ciò che loro occorre. Questo non rende i servizi particolarmente friendly, ne particolarmente piacevoli da utilizzare. La user experience è fondamentale. Le grandi infrastrutture, alcune già realizzate come lo SPID, altre in corso d'opera come l'anagrafe nazionale e il portale dei pagamenti, dovrebbero permetterci di accedere con un profilo personale in un ambiente virtuale dove trovare tutti i servizi e tutte le informazioni ad hoc. La tecnologia lo rende possibile, molto delle infrastrutture citate ci aiutano. È necessario lavorare di più sull'organizzazione degli enti e la collaborazione tra loro, piuttosto che la competizione, questo il salto di innovazione necessaria. Anche per le città metropolitane, c'è un salto di cooperazione intercomunale da fare per condividere i servizi pubblici.

Francesca Bosco, Programme Officer UNICRI – ha parlato nella tavola rotonda di tutela e sicurezza e sviluppo del mercato nell'ambito della ricerca per supportare gli stati membri e identificare le sfide in termini di sicurezza nei programmi di contrasto alla criminalità informatica e a quella organizzata. La mia ricerca è volta non solo a comprendere i rischi, ma anche a valorizzare le possibilità che la tecnologia offre per lo sviluppo e per una società più sicura e più libera. Una volta delle possibili risposte ai problemi vengono dalla rete stessa e da un suo utilizzo consapevole. Lavorare sulle potenzialità e sui rischi del big data analytics è determinante per la sicurezza a livello nazionale e internazionale, dalla prevenzione del crimine al supporto per la gestione dei flussi migratori, dalla biosafety all'intelligenza artificiale.

Alberto Zannol, Amministratore Delegato Mobisec Italia – Privacy e protezione del dato sanitario nell'era del mobile. Il mobile rende possibile nuove capabilities di servizio, di pratica medica e di analisi dei dati di telemedicina grazie a profonde innovazioni tecniche e tecnologiche che si stanno esponenzialmente diffondendo sul mercato. L'urgenza del "time to

market" del servizio però deve pagare lo scotto dei nuovi paradigmi di data acquisition, data exchange e dei relativi nuovi modelli di protezione di privacy, autorizzazione e integrità del dato sanitario, ovunque si trovi ed ovunque venga reso disponibile. La cyber security abbandona il paradigma web classico per approdare ad un nuovo impianto organico e strutturato. Mobisec analizza la sicurezza delle applicazioni mobile di business. Il compito è quello di proteggere i dati del cliente finale ed il business del proprietario dell'applicazione. Troviamo le falle di sicurezza non solo nel codice dell'applicazione, ma anche nella sua interazione con eventuali altre applicazioni, col sistema operativo e con le sorgenti esterne dei dati. A partire dallo studio stesso del prodotto, che vorrebbe declinarsi anche nel segmento della protezione personale del dispositivo (Byod) e alla protezione di informazioni riservate. Dall'altro lato il «sorgente» del software è in fase di sperimentazione anche per applicazioni di servizi alla persona, protezione e gestione dello smartphone ed ottimizzazione della sicurezza del device, nonché alla data acquisition ed al big data qualitativo mobile.

Carlo Borghetti, Componente III Commissione, Sanità e politiche sociali Regione Lombardia – che ha definito questa tematica fondamentale non solo per la vita quotidiana, ma lo è a maggior ragione per il dato sanitario. Il tema della sicurezza e della privacy va di pari passo con la qualità del dato, e quindi bisogna reinvestire negli strumenti informatici per organizzarne la raccolta.

Franco Cornagliotto, Presidente aizoOn – ha fatto un breve cenno sul tema "Wanna cry", un virus informatico ormai famoso in tutto il mondo che ha colpito 105 paesi e oltre 100mila sistemi. A fronte di questi attacchi sempre più frequenti, è necessario non trovarsi impreparati adottando una maggiore sicurezza sui nostri dispositivi. Anche il tema della sanità va rivisto in un'ottica del digitale da un punto di vista della logistica e di accesso alle prestazioni, perché l'impatto che ne deriva è completo. Oggi si è sempre più alla ricerca di un modello sanitario perfetto: il modello di riferimento preso in considerazione dal Presidente aizoOn è quello adottato da Adelaide nel Sud dell'Australia dove si sta cercando di implementare un percorso finalizzato a una migliore organizzazione dal punto di vista logistico e di efficienza nelle prestazioni. Essendo un continente molto popoloso e vasto vi è per l'appunto la necessità di garantire l'accesso a più persone possibili avendo un approccio globale e non solo territoriale. Data la vicinanza con la Cina, Adelaide prende spunto dal loro modello che è caratterizzato dall'utilizzo di tecnologie sempre più innovative.

Nazzareno Di Vittorio, Consulente Giuridico – Investigativo e Analista Digitale Forense – ha parlato di cybersecurity dal punto di vista giuridico partendo dal soggetto inteso come persona fisica, il diretto interessato che si rivolge alla sanità. La gestione dei dati risulta essere ancora difficoltosa. L'informatica forense è una branca della scienza digitale forense legata alle prove acquisite da computer e altri dispositivi di memorizzazione digitale. Il suo scopo, è quello di esaminare dispositivi digitali seguendo processi di analisi forense al fine di identificare, preservare, recuperare, analizzare e presentare fatti o opinioni riguardanti le informazioni raccolte. Questo fa sì che si faccia largo uso di tale scienza nelle indagini riguardanti una varietà di crimini informatici nei quali le prove raccolte, soggette alle stesse pratiche e linee guida di ogni altra prova digitale, saranno usate in ambito di processo. A tal scopo sono utilizzate tecniche e principi legati al recupero dei dati, affiancati però da procedure designate alla creazione di un percorso di revisione e analisi che sia legale. Completa l'esperienza di Di Vittorio, l'attività di formazione di investigazione privata con programmi di studio.

Enzo Veiluva, IT Security Manager CSI Piemonte - La vulnerabilità dei sistemi informatici, oggi riconosciuta a livello globale e le contromisure da approntare, sono stati i temi affrontati dal Manager del CSI. Cittadini, aziende e governi subiscono attacchi sempre più frequenti e difficili da contrastare e il Comitato Interministeriale per la Sicurezza della Repubblica ha recentemente emanato un nuovo provvedimento in tema di Cyber Security al fine di elevare il livello di sicurezza in risposta all'intensificarsi degli attacchi cibernetici contro le infrastrutture del nostro Paese. Tutti dobbiamo diventare parte attiva nella protezione dei dati dei cittadini attraverso un'attività importante di formazione e maturando una maggior consapevolezza e condivisione su questi temi. Per Enzo Veiluva, l'incontro di oggi conferma che le in house possono dare un contributo importante sul tema della sicurezza, condividendo le strategie organizzative, tecnologiche e formative con i propri enti consorziati.

La Tavola Rotonda Privacy del pomeriggio, moderata da **Giorgio Albè**, Avvocato Albé & Associati Studio Legale – ha posto l'attenzione sull'impatto nel settore sanitario del Regolamento Europeo n. 679/2016, applicabile dal 25.05.2018. In particolare sono state esaminate le principali novità introdotte dal Regolamento Europeo ed approfonditi gli adempimenti che le strutture sanitarie (pubbliche e private) dovranno attuare per essere compliant e ridurre al minimo il verificarsi di violazioni dei dati personali. Il tutto nell'ottica di conciliare la tutela della riservatezza dei dati con lo sviluppo delle nuove tecnologie.

Alberto Canadè, Manager di Spike Reply, società specializzata su tematiche di cybersecurity e data protection – A meno di 12 mesi dall'entrata in applicazione del nuovo Regolamento diverse grandi aziende hanno appena iniziato la fase di implementazione del proprio programma GDPR e molte aziende medio-piccole devono ancora iniziare a farlo. Diventa cruciale in un lasso di tempo così breve impiegare al meglio le risorse disponibili per centrare l'obiettivo del 25 maggio 2018, partendo da alcuni punti chiave: redazione del registro dei trattamenti e definizione di una metodologia per la gestione del rischio privacy, ricordandosi altresì che il sistema di gestione della privacy richiesto dal GDPR comporta una revisione del proprio modello organizzativo privacy, e un'azione di sensibilizzazione e informazione trasversale a tutti i livelli aziendali.

Elena Bassoli, Professoressa a contratto di diritto dell'Informatica presso l'Università di Genova, l'Università del Piemonte orientale e la Statale di Milano - L'applicazione, a partire da 25 maggio 2018, del nuovo regolamento europeo sulla privacy (2016/679), che prevede l'obbligo di comunicazione delle violazioni sia al Garante sia agli interessati, ha portato di nuovo in auge negli ultimi mesi argomenti già noti come la cybersecurity, la reputazione aziendale, la necessità di considerare la sicurezza un asset strategico non solo per tutelare l'immagine dell'azienda ma soprattutto per difendere l'operatività del business e le informazioni sensibili riferite ai Clienti. Gli attacchi informatici sono in forte crescita anche in Italia e difficilmente possono essere evitati attraverso politiche difensive individuali. Un'indagine internazionale di Zurich sul rischio di attacchi informatici, elaborata nel 2016 su un campione di oltre 2.600 piccole e medie imprese in 13 paesi del mondo in Europa, America e Asia-Pacifico, rileva che le nostre Pmi sottovalutano ancora i rischi legati al cybercrime rispetto ad altri Paesi. La percentuale di aziende italiane che teme furti di dati dei clienti è quasi la metà della percentuale di aziende irlandesi (21% vs 41%), mentre il timore di essere vittima di un furto di identità è più sottovalutato dalle aziende italiane rispetto alle realtà svizzere (8% vs 19%), e ancora il rischio di furti di denaro in Italia si attesta al 12% contro il 21% degli Usa. Le aziende italiane temono molto di più danni alla reputazione aziendale (17% vs 11,5%), furti di dati dei dipendenti (6,5% vs 5%), furti di denaro (11,5vs 6,5%) e di identità (7,5% vs 3,5%). La comunicazione al Garante e ai singoli interessati è già un obbligo per fornitori di servizi

telefonici e di accesso a internet o per strutture sanitarie, pubbliche amministrazioni e chiunque tratti dati biometrici. Con l'applicazione, dal 25 maggio 2018, del regolamento europeo sulla privacy (2016/679), l'obbligo di comunicare al Garante violazioni di dati personali sarà generalizzato, e riguarderà tutti i casi nei quali le violazioni comportino un "rischio per i diritti e le libertà delle persone fisiche". Inoltre, quando il rischio sia "elevato", sarà obbligatorio informare senza ritardo anche i singoli interessati. Va da sé che tutte le tutte le realtà aziendali, assicurazioni e banche in primis, che trattano dati privati o di importanza strategica debbano adottare misure adeguate per minimizzare l'impatto. In caso di violazione, infatti, avvisare il Garante può permettere di concordare rimedi adeguati e mitigare eventuali sanzioni. Avvisare inoltre gli interessati può contribuire a minimizzare i danni (si pensi al blocco delle carte di credito con numeri violati) a vantaggio della responsabilità del titolare stesso. In altri casi, invece, la comunicazione della violazione può compromettere la fiducia di clienti e mercato, oltre a provocare possibili sanzioni monetarie e blocchi dei trattamenti di dati. Nell'era dei Big Data, di Internet of Things, della pervasività di internet e delle tecnologie che ad esso si appoggiano – device e strumenti che dialogano tra loro attraverso la rete – emerge l'urgenza di focalizzarsi sulle sfide che questo scenario propone e che solo con un adeguato cambiamento culturale si può affrontare con successo.

Roberto Moriondo, Direttore Scientifico Motore Sanità Tech e Direttore Generale Comune di Novara – è partito dalla definizione di cartella sociale e dell'importanza dei dati che la compongono. La cartella sociale permette di conservare i dati inerenti l'intervento di aiuto per ricostruirne l'evoluzione, consente di monitorare l'impiego delle risorse, favorisce la condivisione dei dati all'interno dell'equipe, e agevola il passaggio di informazioni ad altri operatori. Inoltre, è utile alla ricerca in qualità di fonte di informazioni e, non da ultimo, tutela l'utente perché individua impegni assunti a favore dell'utente e i tempi di realizzazione. Il dato sanitario dovrebbe confluire a una trasformazione in diritti e servizi. Nella realtà del comune di Novara di circa 105 mila abitanti, i dipendenti devono quotidianamente gestire i servizi sociali e le politiche per la casa che vedono il dato sanitario come uno degli elementi identificativi del trade off per la gestione dei servizi e la garanzia di diritti.

Secondo **Nicola Ruggiero**, Vicepresidente Anitec – La security dei dati è un aspetto trasversale a tutte le organizzazioni e tutti i sistemi tecnologici che i dati attraversano. Lo sviluppo del mercato deve passare attraverso un forte uso della compliance in tutte le sue forme: è importante darsi delle regole, rispettarle, ma ancora di più farle diventare cultura diffusa di tutti gli operatori che trattano i dati. La tecnologia aiuta a controllare, monitorare, generare, trasportare, imbrigliare e mettere in sicurezza le informazioni, ma rimane l'uomo il vero custode della privacy. Il mercato sanitario ha bisogno più di tanti altri di queste elementari certezze perché tratta aspetti molto intimi e sensibili della nostra vita. Le aziende e le tecnologie ci sono e ci aiutano, ma non c'è miglior privacy e sicurezza di una organizzazione che adotta la cultura giusta e rispetta le regole. Se ciò accade allora l'interscambio dei dati tra le varie organizzazioni interessate favorisce uno sviluppo medico, clinico e commerciale del mercato a vantaggio di tutti, e contribuisce all'efficienza complessiva del sistema sanitario.

Chiara Gallocchio – comunicazione@motoresanita.it - 3278950395