haiku
is cyber intelligence

INSURANCE Daily

VENERDÌ 26 FEBBRAIO 2021 N. 1901

haiku è un marchio di blue underwriting
www.haiku.blue

PRIMO PIANO

Signorini verso l'Ivass

Luigi Federico Signorini sarà il nuovo direttore generale di Banca d'Italia, carica che lo proietterà quindi alla presidenza di Ivass. A seguito della nomina di Daniele Franco a ministro dell'Economia e delle finanze, il consiglio superiore della Banca d'Italia, in seduta straordinaria, su proposta del governatore Ignazio Visco, ha nominato Signorini (già vice dg), direttore generale di Palazzo Koch. La nomina, deliberata ai sensi dell'articolo 18 dello statuto dei Bankitalia, deve essere approvata con decreto del Presidente della Repubblica, promosso dal presidente del Consiglio dei ministri di concerto con il ministro dell'Economia e delle finanze, sentito il Consiglio dei ministri.

Signorini, classe 1955, è entrato nel direttorio di Banca d'Italia come vice direttore generale nel 2013. Durante la sua carriera universitaria è stato assistente di Mario Draghi all'Università di Firenze. Attualmente è membro del Comitato di Basilea, del Board of supervisors dell'Autorità bancaria europea e partecipa ad altri organismi europei e internazionali di coordinamento della vigilanza.

Dopo la crisi del 2008 diventa capo del servizio Normativa e politiche di vigilanza e dà impulso alla normativa sulla trasparenza bancaria. A partire dal 2009, assume la guida del servizio Supervisione sui gruppi bancari.

Fabrizio Aurilia

RICERCHE

Sicurezza informatica, la sfida dell'auto autonoma

Un rapporto realizzato a livello europeo analizza prospettive e rischi delle vetture che sfruttano sistemi di intelligenza artificiale per guidare in maniera indipendente. La minaccia principale arriva da attacchi che possono destabilizzare i modelli di guida. Per questo è necessario sostenere e promuovere una cultura della cyber security

L'errore umano è ancora il principale responsabile di incidenti stradali. Nel 2019, secondo l'ultima edizione del rapporto *Incidenti stradali in Italia* realizzato dall'**Istat**, la distrazione al volante è stata la prima causa di incidenti e collisioni (15,1%), davanti al mancato rispetto del diritto di precedenza (13,8%) e alla velocità elevata (9,3%). In fondo, solo in coda alla graduatoria, si collocano eventi del tutto incontrollabili per l'essere umano, come ostacoli accidentali (2,3%) o irregolarità del manto stradale (0,6%). Ecco perché la prospettiva delle auto a guida autonoma riscuote così tanto successo: eliminando la causa principale di incidenti, ossia il guidatore umano, sarà possibile rendere le strade più sicure per automobilisti, passeggeri e pedoni. Peccato però che, così facendo, si incorra in altri motivi di rischio. A cominciare da una sicurezza dei sistemi di guida autonoma che, almeno per il momento, non può essere garantita.

L'ultimo monito in questo ambito è arrivato dal rapporto *Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving*, realizzato da European Union Agency for Cybersecurity (**Enisa**) e dal Joint Research Centre (**Jrc**). Il rapporto, come si intuisce già dal titolo, si focalizza in particolare sui sistemi di intelligenza artificiale delle auto a guida autonoma. "Le auto autonome utilizzano sistemi di intelligenza artificiale che impiegano tecniche di machine learning per raccogliere, analizzare e trasferire dati, al fine di prendere quelle decisioni che nelle auto convenzionali vengono prese dall'uomo", si legge nella ricerca. "Questi sistemi, come del resto qualsiasi altro sistema informatico, sono vulnerabili ad attacchi – prosegue il rapporto – che possono compromettere il corretto funzionamento del veicolo". Ossia, detto in altri termini, provocare incidenti stradali. E azzerare così quasi completamente il vantaggio principale delle auto in grado di guidare da sole.

(continua a pag. 2)

INSURANCE REVIEW È SU TWITTER
Seguici cliccando qui
INSURANCE REVIEW

(continua da pag. 1)

AUTO SOTTO ATTACCO

Il settore delle auto a guida autonoma, anche sulla scia dei traguardi raggiunti dai sistemi di intelligenza artificiale in altri ambiti, è cresciuto moltissimo negli ultimi anni. I prototipi sono in grado di riconoscere i segnali stradali e la segnaletica orizzontale della carreggiata, rilevare la presenza di ostacoli o altri veicoli, stimarne la velocità e pianificare così la strada da percorrere. Eppure il rischio di errore, anche per una macchina, è sempre in agguato: negli ultimi anni ci sono stati vari casi di incidenti, talvolta anche drammatici, dovuti a malfunzionamenti dei sistemi di guida autonoma.

A ciò si aggiunge poi il rischio di attacchi intenzionali volti a interferire con i sistemi di intelligenza artificiale ed eludere i protocolli di sicurezza. "Pattern realizzati con cura possono essere disseminati nell'ambiente per alterare i processi decisionali della vettura e indurre comportamenti inaspettati", si legge nel rapporto. "Gli esempi tipici – prosegue la ricerca – sono l'alterazione della segnaletica orizzontale per fuorviare i sistemi i navigazione o l'applicazione di un adesivo su un segnale di stop per impedirne il riconoscimento". Altri rischi vengono da attacchi DoS/DDoS o da intrusioni volte a manipolare i canali di comunicazione del veicolo. Seppur non strettamente collegata alla sicurezza della vettura, c'è poi da considerare anche la possibilità di attacchi volti a sottrarre i dati raccolti dai sistemi di intelligenza artificiale.

UNA CULTURA DELLA SICUREZZA INFORMATICA

Per quanto complessi da realizzare, attacchi di questo genere restano possibili. Di conseguenza, scrivono i ricercatori, "le terribili conseguenze in termini di sicurezza dovrebbero spingere le case produttrici a mettere in atto meccanismi di difesa per mitigare i rischi connessi all'intelligenza artificiale". L'industria nel suo complesso "dovrebbe abbracciare un approccio di security by design per lo sviluppo e l'impiego delle funzionalità di intelligenza artificiale: ciò includerebbe l'utilizzo di modelli standardizzati e soluzioni omogenee interoperabili". È importante, secondo il rapporto, "promuovere una cultura della sicurezza informatica in tutto l'ecosistema dell'auto, sviluppando best practics, spingendo l'innovazione e integrando progressivamente i controlli di cybersecurity negli attuali processi industriali connessi al ciclo di vita delle auto a guida autonoma".

(continua a pag. 3)

LEGGE
FINANZIARIA 2021

BONUS
PUBBLICITÀ
50%

PUOI RECUPERARE IL 50%
DEGLI INVESTIMENTI
PUBBLICITARI SU TUTTI
I NOSTRI STRUMENTI

PER INFORMAZIONI
CLICCA QUI

haiku
is cyber intelligence

INSURANCE Daily

VENERDÌ 26 FEBBRAIO 2021 N. 1901

haiku è un marchio di blue underwriting
www.haiku.blue

(continua da pag. 2)

Una cultura della sicurezza informatica sarà fondamentale anche in ambito legislativo, in tutto il panorama europeo. "È importante che la regolamentazione europea assicuri che i benefici delle auto autonome non siano annullati dai rischi per la sicurezza", ha commentato Stephen Quest, direttore generale del Jrc. Anche perché, come ha ricordato **Juhan Lepassaar**, executive director dell'Enisa, "quando una pericolosa auto a guida autonoma attraversa il confine di uno Stato membro dell'Unione Europea, porta con sé tutte le sue vulnerabilità: la sicurezza non deve essere posta in secondo piano, ma un impiego affidabile di questo genere di veicoli sulle strade europee deve essere invece un prerequisito".

RACCOMANDAZIONI AL MERCATO

Il rapporto si conclude con una serie di raccomandazioni al mercato. Si tratta soprattutto di osservazioni di buon senso, consigli utili più a focalizzare l'attenzione sulla sicurezza delle soluzioni che a definire veri e propri modelli operativi. Si parte da processi di security assessment e si arriva a schemi di validazione dei modelli di intelligenza artificiale e dei sistemi di raccolta ed elaborazione dati, passando per lo sviluppo di meccanismi di resilienza e l'elaborazione di piani di gestione di eventuali incidenti. Particolare attenzione è posta poi sulla condivisione di standard lungo l'intera supply chain, visto che la maggior parte delle case si affida a fornitori esterni per le componenti elettroniche: per questo il rapporto suggerisce di stabilire una chiara politica di sicurezza lungo tutta la catena di fornitura, assicurarne il rispetto, identificare le potenziali fonti di rischio e richiedere anche i fornitori il rispetto della normativa prevista per l'industria automobilistica. Più in generale, il rapporto invita il settore a sviluppare e diffondere una cultura della sicurezza focalizzata sull'intelligenza artificiale. Solo così sarà possibile avere davvero, prima o poi, auto in grado di guidarsi da sole sulle nostre strade.

Giacomo Corvi

ANIA

Ue: più coperture assicurative per fronteggiare le Nat-Cat

L'Ania plaude alla proposta della Commissione di una nuova strategia comunitaria sul clima, che prevede un maggior coinvolgimento del settore assicurativo

L'**Ania** rinnova la sua proposta per un sistema gestionale pubblico-privato sulle catastrofi naturali in Italia. L'associazione delle imprese assicurative ha voluto commentare la proposta, avanzata nei giorni scorsi dalla Commissione europea, per una nuova strategia comunitaria sull'adattamento ai cambiamenti climatici, e per fronteggiare gli effetti degli eventi catastrofali.

Tra le molte linee d'azione suggerite, l'Ania ha voluto mettere l'accento su quella volta a colmare il "gap di protezione climatica" determinato dalla parte dei costi derivanti dalle catastrofi naturali non coperta da un'assicurazione. La Commissione sottolinea che oggi tale copertura, a livello europeo, va da un minimo del 5% a un massimo del 35% del totale dei danni, mentre l'industria assicurativa ha calcolato che ogni punto percentuale in più di copertura potrebbe ridurre i costi globali a carico della fiscalità generale del 22%.

"Ecco perché la Commissione europea – scrive l'Ania in un comunicato – preconizza di includere pienamente questo aspetto nella strategia di lotta ai cambiamenti climatici, di promuovere il più possibile schemi assicurativi nazionali contro le catastrofi naturali e di potenziare il lavoro di monitoraggio e coordinamento già in corso a livello Ue, annunciando la sua intenzione di avviare un dialogo approfondito con le parti interessate a partire dalle imprese assicuratrici".

Commentando la strategia europea, la presidente di Ania, **Maria Bianca Farina**, ha detto di apprezzare le proposte della Commissione europea, e in particolare il rilievo e il valore del ruolo assegnato al settore assicurativo nella mitigazione degli effetti delle catastrofi naturali. "La proposta – ha spiegato Farina – va nel senso da sempre auspicato da Ania di perseguire una più efficace resilienza agli eventi catastrofali, con la conseguente riduzione dei costi a carico dello Stato per la copertura dei loro effetti".

L'associazione auspica la realizzazione anche in Italia di "un sistema gestionale, programmato ex ante ed efficiente del rischio derivante dalle catastrofi naturali attraverso una partnership pubblico-privata che preveda – tra le altre iniziative – uno strumento di assicurazione delle abitazioni private contro i rischi connessi a terremoti, alluvioni ed eventi naturali". Facendo leva sulla mutualizzazione assicurativa dei rischi, aggiunge Ania, "si possono garantire prezzi contenuti, tempi certi e ragionevoli di risarcimento del danno, trasparenza nelle procedure, con attenzione rigorosa alla prevenzione, opportune modalità di finanziamento della ricostruzione e ottimizzazione della gestione delle emergenze post-evento".

B.M.

haiku
is cyber intelligence

INSURANCE Daily

VENERDÌ 26 FEBBRAIO 2021 N. 1901

haiku è un marchio di blue underwriting
www.haiku.blue

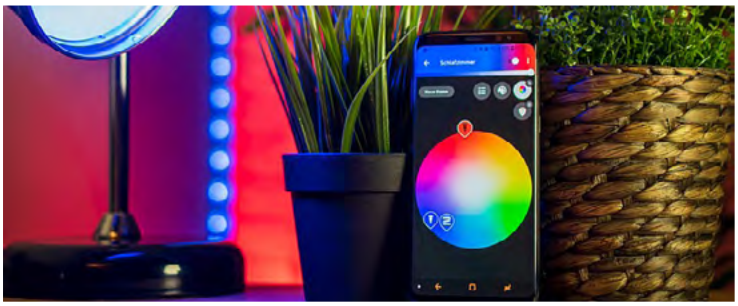
RICERCHE

Cambiano i trend della smart home

In un contesto che nel 2020 ha visto un calo di interesse complessivo, perdono di più le soluzioni per la sicurezza della casa e aumentano gli speaker. È possibile che il mercato abbia risentito degli effetti della pandemia, perché altri elementi fanno pensare a una rinnovata crescita, ma su basi differenti

Le soluzioni della *smart home* crescono in interesse tra gli italiani, anche se lo scorso anno ha visto cambiamenti di approccio al settore che potrebbero segnare una svolta forse definitiva. Il tema della casa intelligente è noto al 69% dei consumatori del nostro Paese, con percentuali più alte nella fascia di età 18-34 anni (82%) e tra chi è più avvezzo alle tecnologie (89%); il 43% possiede almeno un oggetto smart e due persone su tre dichiarano di utilizzare con frequenza queste tecnologie, mentre riguardo all'utilizzo delle funzionalità il 19% afferma di averne aumentato l'uso contro il 13% lo ha ridotto.

I risultati dell'*Osservatorio Internet of Things* della **School of Management del Politecnico di Milano**, presentati nel corso del convegno online *Stay at home, stay in a Smart Home: la casa intelligente alla prova del Covid*, mostrano una diversa consapevolezza verso le potenzialità delle soluzioni smart, sempre meno gadget tecnologico e sempre più strumento di concreta utilità. Lo scorso anno, e l'esperienza della pandemia non ne è estranea, è calato l'interesse verso gli oggetti intelligenti (il 14% li ritiene meno prioritari rispetto a prima del Covid, contro il 4% che ne accredita maggiore utilità) e, tra chi intende effettuare acquisti in questo ambito, il 28% ha ridotto il budget disponibile mentre il 5% lo ha aumentato. È possibile però che si tratti di un dato transitorio, influenzato dalla particolare esperienza dell'emergenza: i mesi di restrizione negli spostamenti hanno, al contrario, fatto crescere due trend affini al mercato della smart home, cioè l'interesse per la cura della casa e l'utilizzo delle tecnologie. Certamente nell'ultimo periodo è evoluto l'approccio verso le tecnologie smart, che vengono considerate di più per le loro reali potenzialità: dalle risposte raccolte, il 62% degli intervistati sarebbe interessato, in prospettiva, ad acquistare almeno un servizio associato ai dispositivi connessi e circa un terzo si dice disposto a pagare di più per l'attivazione, soprattutto se si tratta di servizi di assistenza medica (35%) e di monitoraggio e ottimizzazione dei consumi energetici (31%).



Verso una consapevolezza del prodotto

Il 2020 ha visto una riduzione dell'interesse dei consumatori verso le soluzioni smart per la sicurezza dell'abitazione, che rimane comunque la prima voce nelle quote di mercato (21%) ma con un calo del 30% rispetto al 2019; in parallelo, l'interesse dichiarato per l'acquisto di queste tecnologie vede come prima motivazione sempre la sicurezza, ma in calo dal 36% al 27%. Cresce invece la quota di mercato degli *smart home speaker*, che eguagliano le tecnologie per la sicurezza al 21%, con una crescita del 10% nei 12 mesi: punto debole, secondo l'Osservatorio, rimane l'integrazione di questi sistemi con gli altri oggetti smart presenti in casa, potenzialità utilizzata solo dal 14% di chi li ha acquistati.

Per quanto riguarda i canali di vendita, in un contesto complessivo che ha visto il mercato ridursi del 5% (in totale vale 505 milioni di euro), il retail online è cresciuto del 20% e copre ora una quota di mercato del 36%; tutti gli altri canali professionali hanno segnato il passo (il canale tradizionale è passato dal 50% del 2018 al 34% del 2020) mentre sono rimaste contenute le vendite da parte di telco, utility e compagnie assicurative.

Maria Moro

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 26 febbraio di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577