Rassegna stampa

Centro Studi C.N.I. 22 gennaio 2017

Waypress
media monitoring

MAPPA SISMICA

INGV

PROTEZIONE CIVILE

CONCORRENZA

CYBERSECURITY

Il Sole 24 ORE

Mappa sismica bloccata, bonus ancora fermo

I ritardi del Consiglio superiore dei lavori pubblici rendono inapplicabile la maxiagevolazione

Giuseppe Latour
ROMA

Sismabonus non pervenuto. Il principale strumento di incentivazione alla messa in sicurezza antisismica dell'ultima legge di Bilancio, per adesso, è in larga parte un guscio vuoto. Guardando all'ampio set di sconti disegnato dalla manovra, infatti, dal primo gennaio scorso si è messa in moto solo la detrazione con i giri più bassi, quella del 50 per cento. La vera fuoriserie del nuovo sistema è la maxi agevolazione compresa tra il 70 e l'85%: nonostante le promesse, è ancora inattuata. Per mandarla in pista servirebbe una linea guida per la mappatura degli edifici che, al momento, è ferma al Consiglio superiore dei lavori pubblici, il massimo organo consultivo dello Stato. L'impegno di completarla entro fine anno è stato mancato. La prossima scadenza è fissata a fine febbraio ed è ad alto rischio. Un ritardo incredibile, visto che una bozza del provvedimento è pronta almeno da maggio del 2016.

Per capire cosa si sta inceppando, partiamo dalla manovra. La legge di Bilancio 2017 disciplina il nuovo sismabonus, relativo alle spese sostenute per la messa in sicurezza degli edifici. È attivo fino al 2021 ed è strutturato in due blocchi. Il primo livello è una detrazione del 50 per cento. Si applica non solo agli edifici in zone sismiche ad alta pericolosità (zone 1 e 2), ma anche a quelli in zona sismica 3. Questo, che è già attivo, è il blocco meno interessante, perché garantisce la stessa aliquota delle ristrutturazioni ordinarie (il 50%), con il solo vantaggio di avere un tempo di detrazione inferiore: cinque anni, anziché dieci. Il vero perno del sismabonus è il secondo livello. Qualora dagli interventi «derivi una riduzione del rischio sismico che determini il passaggio ad una classe di rischio inferiore, la detrazione di imposta spetta nella misura del 70 per cento», spiega la relazione illustrativa della manovra. Con due classi di rischio in meno, si arriva all'80 per cento. Addirittura, se l'intervento riguarda parti comuni dei condomini, si ottiene un beneficio di altri cinque punti: il tetto massimo, in sostanza, è ben 85 per cento. Che, però, per adesso è solo sulla carta.

L'OBIETTIVO MANCATO
Le linee guida per la mappatura degli edifici erano attese entro dicembre 2016. Ma adesso sembra a rischio anche la scadenza di fine febbraio

LA PAROLA CHIAVE

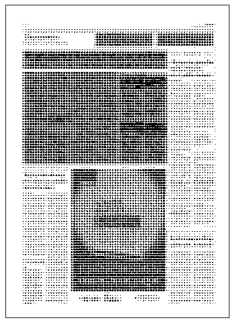
Zone a rischio sismico

● Il territorio italiano è diviso, a partire dal 2003, in quattro zone, a seconda del livello di pericolosità sismica e della storia delle aree. La zona «1» è la più pericolosa: qui possono verificarsi terremoti definiti "fortissimi". Alto il rischio anche nella zona «2», mentre nella zona «3» eventi catastrofici possono verificarsi, ma sono rari. L'ultima zona, quella meno pericolosa, è infine la «4». Qui i terremoti, anche di scarsa intensità, sono poco frequenti.

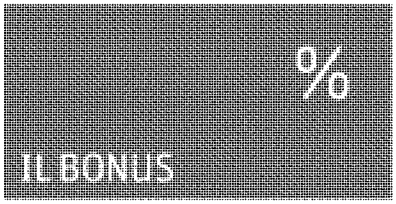
Il motivo è che il sistema delle classi di rischio deve essere regolato da un decreto del ministero delle Infrastrutture, da adottare dopo avere sentito il Consiglio superiore dei lavori pubblici. Questo provvedimento manderà a regime un metodo di mappatura degli edifici assimilabile a quello degli elettrodomestici: a seconda dello stato dell'immobile, si otterrà una lettera dalla A alla F e, con gli interventi di messa in sicurezza, si potrà ottenere un salto di classe e, quindi, uno sconto fiscale. Senza le regole per la mappatura, il bonus resta un guscio vuoto. E, almeno per ora, le regole per la mappatura sono incagliate.

La manovra, per la verità, fissa il limite di fine febbraio per l'attuazione della norma. Ma l'andamento dei lavori in Consiglio superiore fa immaginare che si andrà oltre questo termine. Inoltre, lo stesso Consiglio superiore aveva annunciato, nel mese di ottobre, che avrebbe chiuso il dossier a fine 2016, in modo da far partire il bonus già a gennaio del 2017. Le premesse per farlo c'erano tutte: la bozza delle linee guida, infatti, era già pronta da diversi mesi. Un po' di storia recente aiuta a capire cosa sta accadendo. La scrittura di queste linee guida inizia a ottobre del 2013: all'epoca si trattava di un meccanismo sperimentale di classificazione degli edifici, da aggiornare eventualmente a un nuovo sistema di bonus fiscali. A guidare la commissione di esperti incaricata di elaborare il testo era Pietro Baratono, provveditore alle Opere pubbliche di Lombardia ed Emilia Romagna. Il lavoro a maggio 2016 risultava chiuso, perché lo stesso Mit rispondeva a un'interrogazione presso la commissione Ambiente della Camera, spiegando che il gruppo di studio aveva «elaborato» le linee guida e che queste «verranno a breve rese pubbliche». All'epoca – va detto – non esistevano gli sconti fiscali che ci sono ora, quindi la loro pubblicazione poco avrebbe cambiato in termini di prevenzione.

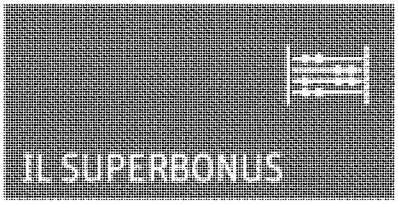
La sostanza, però, è che dopo l'estate il Governo ha iniziato a disegnare il sismabonus, forte di una linea guida già quasi pronta all'uso. Il Consiglio superiore, però, la pensava diversamente e ha così messo un tappo al sistema di mappatura dei fabbricati, per motivi di carattere tecnico: il vecchio testo, infatti, era organizzato sulla base di criteri economici di classificazione del rischio sismico. Il nuovo, secondo l'orientamento emerso in sede di revisione, dovrà mettere al centro la salvaguardia delle vite umane. Al di là del merito scientifico, si è deciso di procedere a un'ampia rimodulazione del provvedimento. Così, per il maxi sconto dell'85% bisognerà aspettare ancora. La previsione, se tutto andrà bene, è di chiudere la parte del Consiglio superiore entro febbraio. Approvare poi il decreto nel giro di pochi giorni, come previsto dalla manovra, a quel punto sarà molto complicato.



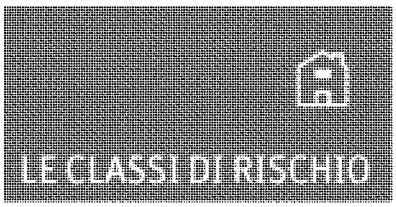
Come funziona il sismabonus



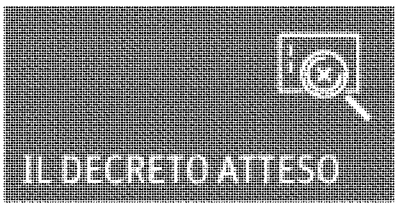
La detrazione è al 50%
È il primo livello di agevolazione già in vigore. Si applica non solo agli edifici in zone sismiche ad alta pericolosità (1 e 2), ma anche a quelli in zona sismica 3. Questo bonus garantisce la stessa aliquota delle ristrutturazioni ordinarie (il 50%), con il solo vantaggio di avere un tempo di detrazione inferiore: cinque anni, anziché dieci



Detrazione fino all'85%
Il secondo livello - non ancora attuato - prevede che se dagli interventi derivi una riduzione del rischio sismico con il passaggio ad una classe di rischio inferiore, la detrazione di imposta è al 70%.. Con due classi di rischio in meno si arriva all'80 % e se l'intervento riguarda parti comuni dei condomini, si ottiene il tetto massimo all'85%



Come negli elettrodomestici
L'introduzione delle classi di rischio prevede un metodo di mappatura degli edifici che è assimilabile a quello utilizzato per gli elettrodomestici: a seconda dello stato dell'immobile, si otterrà una lettera dalla A alla F e, con gli interventi di messa in sicurezza, si potrà ottenere un salto di classe e, quindi, uno sconto fiscale.



Le norme attese entro febbraio
Manca all'appello il metodo di mappatura delle classi di rischio che deve essere regolato da un decreto del ministero delle Infrastrutture, da adottare dopo avere sentito il Consiglio superiore dei lavori pubblici. La manovra fissa il limite di febbraio per attuare la norma. Ma l'andamento dei lavori in Consiglio superiore fa immaginare che si andrà oltre

L'incentivo già attivo

Finora è potuta partire solo la detrazione meno appetibile: quella del 50% spalmata su 5 anni

L'agevolazione inattuata

Al momento non è ancora utilizzabile lo sconto compreso tra il 70 e l'85% degli interventi

I fondi. Ogni anno 50 milioni, l'80% per gli stipendi

Ingv senza risorse per ricerca e studio sui terremoti

Marzio Bartoloni

Cinquanta milioni all'anno, di cui 40 servono per pagare gli stipendi, per fare la ricerca su terremoti (e vulcani) in Italia, l'ottavo Paese al mondo più colpito negli ultimi 15 anni. Queste le risorse a disposizione del nostro Istituto nazionale di geofisica e vulcanologia, l'Ingv, una sigla che gli italiani purtroppo hanno imparato a conoscere molto bene perché è da lì che arrivano i tweet con la stima della magnitudo e della profondità di ogni scossa. Ma dietro a questa sigla c'è anche uno dei nostri più importanti enti di ricerca a cui il Miur ogni anno assegna il finanziamento per la sua attività attraverso il riparto del Foe (il Fondo ordinario degli enti). Un'assegnazione che l'anno scorso è stata di 55 milioni, praticamente le stesse risorse che l'Ingv riceveva 10 anni fa (54 milioni nel 2007).

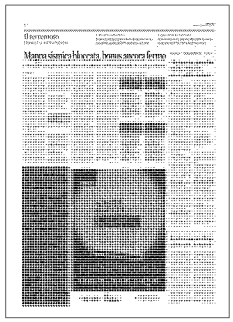
«Purtroppo i finanziamenti assegnati all'Ingv sono insufficienti per farlo vivere, siamo in bolletta», è l'appello lanciato dal presidente dell'Istituto, Carlo Doglioni, in piena emergenza terremoto negli appennini monitorati costantemente dalla rete di 300 sismografi della rete nazionale che fa capo all'Ingv a cui si aggiungono quelli delle stazioni mobili, le ricerche sul campo e l'analisi delle immagini rilevate dai satelliti. Conoscenze indispensabili, queste, per riuscire a conoscere a fondo il comportamento del suolo in un Paese sismico come l'Italia e, forse, per arrivare un giorno a conquistare quella sorta di Sacro Graal della sismologia che è la possibilità di prevedere un terremoto, ossia poter dire esattamente quando e dove la terra tremerà: cosa oggi assolutamente impossibile. «È talmente importante studiare la Terra - ha aggiunto Doglioni - che non si capisce perché non si voglia investire di più per capire come funziona il nostro pianeta». Ma portare avanti progetti di ricerca in questo momento è davvero molto difficile perchè «i fondi dell'Ingv non bastano a coprire le spese, non riusciamo a pagare gli stipendi e il mantenimento delle strutture e non abbiamo soldi per i progetti di ricerca». Secondo i dati diffusi dal Miur a fine 2015 il 79% dei fondi assegnati servivano per pagare gli stipendi a personale e ricercatori. Il resto basta a pagare le spese di mantenimento delle 26 sedi e poi le briciole per la ricerca. Per Doglioni «un ente normale deve avere un bilancio che permetta di fare ricerca e noi abbiamo per questo già lanciato un importante progetto per lo studio della terra, "working earth", a cui basterebbe un finanziamento del 10% del nostro bilancio »: oggi invece l'Ingv su circa mille dipendenti conta 400 precari, «150 delle quali sono ricercatori a tempo determinato, che non sanno che succederà a fine contratto». Con l'ultimo decreto sugli enti di ricerca (in attuazione della riforma Madia) che ha previsto un paletto preciso: chi ha un costo del personale che vale l'80% del bilancio non può assumere.

IL BILANCIO

55

I milioni assegnati all'Ingv

Nel riparto del Fondo ordinario degli enti di ricerca dell'anno scorso (l'ultimo) il ministero dell'Istruzione, Università e Ricerca ha previsto una assegnazione complessiva di 55 milioni. Da 10 anni le risorse sono più o meno le stesse: nel 2015 e 2014 sono state 51 milioni, 49 milioni negli anni dal 2011 al 2013. E poi 57 nel 2010, 61 milioni nel 2009, 59 milioni nel 2008 e 54 nel 2007. Oggi su circa mille dipendenti, 400 sono precari, di cui 150 ricercatori a tempo determinato



Le misure allo studio. Curcio non è in discussione ma a breve partirà il confronto tra Palazzo Chigi, Interno e Difesa su meccanismi e procedure di soccorso e di intervento

E il governo studia la Protezione civile 3.0

Marco Ludovico
ROMA

La riflessione nel governo è già in corso. L'angoscia per la sorte dei 23 dispersi dell'hotel Rigopiano diventa, con il trascorrere delle ore, un incubo. Se le cifre dei morti saliranno, com'è scontato, la tragedia imporrà una risposta politica. L'invio sul posto del viceministro dell'Interno, Filippo Bubbico, deciso dal presidente del Consiglio Paolo Gentiloni e dal titolare del Viminale, Marco Minniti, è un segnale iniziale. Ma tra palazzo Chigi e l'Interno, soprattutto, ma anche il dicastero della Difesa, guidato da Roberta Pinotti, partirà a breve un confronto su meccanismi e procedure di soccorso e di intervento. Da migliorare. Non sono più ammissibili buchi nella catena informativa, com'è accaduto per l'albergo di Farindola, in caso di disastro o di minaccia. E anche un evento straordinario come una nevicata fino a due-tre metri di altezza non può essere subìto fino a portare decine di Comuni all'isolamento. Un fatto è certo: il capo della Protezione civile, Fabrizio Curcio, non è affatto in discussione. Curcio ha lavorato a fianco di Franco Gabrielli, che poi ha lasciato la Protezione per la prefettura di Roma e oggi è alla guida del dipartimento di Ps.

Quella di oggi non è la Protezione civile di Guido Bertolaso, efficiente certo ma poi diventata abnorme fino a occuparsi di grandi eventi e appalti, con tanto di conseguenze giudiziarie. Il potere di coordinamento degli interventi, affidato a Curcio, finora non ha trovato critiche determinanti, anzi i riconoscimenti sono continui. Emerge tuttavia sempre più spesso come il teatro degli attori sul palcoscenico abbia figure a volte scolorite. Se non assenti. Le conseguenze ricadono sul regista Curcio. I Comuni, le Province e le Regioni sono terminali fondamentali del sistema di protezione e difesa civile. Se si abbatte una calamità, le prime informazioni arrivano proprio dal territorio colpito. I "piani neve" devono essere approntati e ne mancano molti, invece, nelle zone ora colpite. La sottovalutazione degli allerta meteo, inviati quasi ogni giorno dagli uffici di Curcio, fa scalpore. Non solo per le carenze sulle iniziative di prevenzione. Ma anche per gli obblighi degli enti locali in questa vicenda. La macchina dei soccorsi dimostra ancora una volta capacità straordinarie con tutte le forze impegnate, Vigili del Fuoco ed Esercito italiano in testa, ma anche Carabinieri, Polizia di Stato e Guardia di Finanza. Nell'esecutivo, tuttavia, e al Viminale in particolare, ci si interroga sulla tenuta e l'incisività dell'azione delle prefetture: va ricordato che il loro nuovo nome – quasi mai usato in realtà – è utg, uffici territoriali del governo. Nelle regioni interessate dal terremoto le prefetture devono essere terminali di un'azione di coordinamento e di monitoraggio continuo delle criticità in atto. Ma forse non è avvenuta a dovere, ad esempio, sulle condizioni di viabilità o sull'erogazione dei servizi pubblici essenziali come l'elettricità. In Abruzzo come in altre zone.

Certo le inchieste già in corso delle procure della repubblica accerteranno alcune responsabilità nei disastri come quello dell'albergo Rigopiano. Ma la questione non può essere risolta da una o più indagini giudiziarie. Né con un'aggiunta di risorse agli enti territoriali per dotarli di più mezzi di soccorso. Le previsioni meteo per l'inverno, ma anche le analisi dei sismologi, sono allarmanti. Aggiornamento e garanzie massime di efficienza del sistema di soccorso e di protezione civile diventano una priorità politica. Un tema in aggiunta a sicurezza e immigrazione nell'agenda del ministro Minniti in audizione mercoledì prossimo a Montecitorio.

SUL TERRITORIO
Monitoraggio sull'azione di prefetture ed enti territoriali L'obiettivo è eliminare i buchi nelle comunicazioni su condizioni meteo e viabilità

LE MISURE

I ministeri coinvolti
Tra palazzo Chigi e ministero dell'Interno Interno, soprattutto, ma anche il dicastero della Difesa, guidato da Roberta Pinotti, partirà a breve un confronto su meccanismi e procedure di soccorso e di intervento. Da migliorare. Non sono più ammissibili buchi nella catena informativa, com'è accaduto per l'albergo di Farindola

Le strutture sul territorio
Nell'esecutivo, tuttavia, e al Viminale in particolare, ci si interroga sulla tenuta e l'incisività dell'azione delle prefetture. I Comuni, le Province e le Regioni sono terminali fondamentali del sistema di protezione e difesa civile. I "piani neve" devono essere approntati


A Rigopiano si scava ancora, Il superstiti

Consumatori. Dal 3 febbraio si ampliano gli strumenti a disposizione per contrastare le pratiche scorrette degli operatori

Concorrenza, tutela in Tribunale

I privati potranno rivolgersi ai giudici delle sezioni speciali per il risarcimento del danno

Guglielmo Saporito

Consumatore al centro dell'attenzione del governo con l'entrata in vigore (il prossimo 3 febbraio) del **decreto legislativo 3/2017** (pubblicato sulla Gazzetta ufficiale del 19 gennaio) riguardante il risarcimento danni per violazione del diritto della concorrenza.

Il Trattato dell'Unione europea condanna le **pratiche concordate che limitano la concorrenza, nonché gli abusi di posizione dominante**. Di tali problemi si sono occupate sinora le diverse **autorità garanti** (si veda la "parola chiave" qui sotto) e dal 2017, con una norma di chiusura, si occuperanno anche i **giudici ordinari** in sezioni speciali a Milano, Roma e Napoli. A tali giudici potranno rivolgersi i consumatori, cioè i privati, singolarmente o in azioni di classe.

I vari tipi di illeciti concorrenziali e gli abusi di posizione dominante non sono descritti nella norma del 2017, ma sono ricostruibili scorrendo le varie indagini e i provvedimenti sanzionatori emessi dalle Autorità garanti. È anche possibile che più Autorità si ritengano competenti a sanzionare lo stesso comportamento anticoncorrenziale di un'unica impresa, come di recente capitato a Wind. L'impresa è stata sanzionata per 200.000 euro per aver collocato sul mercato Sim telefoniche preimpostate a danno del consumatore, e su tale comportamento sia Agcm che Agcom hanno iniziato indagini e previsto sanzioni, con un conflitto che il Consiglio di Stato (167/2017) ha poi affidato alla Corte di giustizia europea.

Ai provvedimenti sanzionatori delle varie Autorità, espressione di "public enforcement" (sanzioni pubblicistiche, che vengono incamerate dallo Stato), si aggiungono ora quelli richiesti da privati (singoli o come classe), con azioni di "private enforcement" (rimedi privatistici, con risarcimenti ai privati). In questo modo i canali di tutela pubblicistico (di spettanza delle Autorità garanti) e privatistico, legato al diritto dei privati, interagiscono per dissuadere le imprese da comportamenti anticoncorrenziali. Non sono solo (come nei casi più recenti) i produttori di cemento, gli operatori telefonici, i gestori di distributori automatici o i produttori televisivi a dover temere questa nuova e più complessa situazione: potranno essere presi di mira anche le associazioni di settore (industria, commercio, servizi) e gli stessi ordini professionali.

Appena pochi giorni fa (11 gennaio) l'Antitrust ha aperto un'istruttoria sul Consiglio notarile di Milano perché, attraverso un controllo sull'attività dei professionisti, avrebbe individuato soglie massime di attività (numero di rogiti), limitando le capacità di ottimizzare i fattori del lavoro, la concorrenza tra professionisti e incidendo sui costi per i consumatori.

Con l'entrata in vigore del decreto legislativo 3/2017 si delineano quindi inedite alleanze tra Autorità garanti e privati litiganti (che si sentano danneggiati), singoli o in formazioni collettive. Le autorità metteranno a disposizione i loro dati, frutto di specifica capacità di ispezione (che dispone anche della Guardia di finanza), mentre i singoli apporteranno il loro contributo di conoscenza delle difficoltà del mercato in caso di intesa anticoncorrenziale.

Inoltre, in presenza di pratiche escludenti, prezzi predatori, clausole fidelizzanti, dinieghi di accesso a infrastrutture essenziali (cioè degli abusi più frequenti), le Autorità possono irrogare sanzioni quantificate con scenari ipotetici o partendo da dati di bilancio, mentre i privati che riterranno di litigare potranno fornire propri dati ed elementi di prova (il tempo e le iniziative perse, i rifiuti subiti).

Nei tribunali di Milano, Roma e Napoli, il risarcimento potrà essere chiesto anche dagli "acquirenti indiretti", cioè da chi non abbia avuto alcun rapporto commerciale con l'autore dell'infrazione, ma abbia comunque subito un "danno per traslazione".

Solo le piccole e medie imprese (quali definite dalla raccomandazione 2003/361/Ce) avranno un regime agevolato, perché (articolo 9 del Dlgs 3/2017) rispondono solo dei danni patiti dai loro acquirenti diretti e indiretti (e non dei danni subiti da altri danneggiati): ciò, tuttavia, sempre che la Pmi abbia una quota del mercato rilevante inferiore al 5% oppure quando il generale principio della responsabilità solidale (che colpisce allo stesso modo di tutti gli operatori che hanno operato in modo anticoncorrenziale) pregiudicherebbe la solidità economica della piccola impresa.

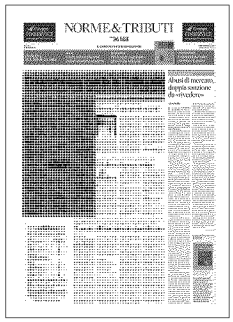
LE SEDI

Le cause potranno essere presentate a Milano, Roma e Napoli, anche da chi non ha avuto rapporti commerciali diretti con l'accusato

LA PAROLA CHIAVE

Autorità garante

- Oltre alla Commissione Ue sono autorità garanti della concorrenza, secondo il contesto:
- Agcm, Autorità garante concorrenza e mercato, chiamata anche antitrust; l'Autorità è composta da 3 componenti, di cui uno è il presidente;
- Agcom, Autorità per le comunicazioni; il Consiglio è composto dal presidente più 4 commissari;
- Aeegsi, Autorità per l'energia elettrica, il gas e il sistema idrico: un presidente e 4 membri del Collegio
- Art, Autorità di regolazione dei trasporti retta da un organo collegiale con un presidente e 2 componenti


NORME&TRIBUTI

Protezione dei dati | Politica industriale | Strategia e ritardi

Il paradosso italiano tra digitale e sicurezza

Il piano «Industria 4.0» offre alle aziende una netta occasione per investire in innovazione. Più fosca la visione sulla cybersecurity

di **Alessandro Longo**

Una industria nazionale innovativa deve essere anche cyber sicura, gli esperti sono concordi; ma su questo punto l'Italia sta procedendo con uno strabismo che non ha pari nella storia del digitale. Da una parte, «abbiamo probabilmente, con l'ultima Legge di Bilancio, il piano Industry 4.0 più completo in Europa», dice Andrea Bianchi, direttore Politiche Industriali di Confindustria. Dall'altra, abbiamo anche il piano cybersecurity più misero tra i grandi Paesi europei, per risorse impiegate e ampiezza della strategia.

Il paradosso è emerso durante l'evento Itasec questa settimana, a Venezia, e sarà toccato il 25 gennaio a Roma all'Industry 4.0 Summit alla Camera dei Deputati. «Piano Industry 4.0 e strategia cybersecurity devono viaggiare di pari passo, altrimenti quelli del piano non saranno solo investimenti sprecati, ma rischiano persino di trasformarsi in un boomerang per le aziende», riassume Paolo Prinetto, presidente del Cini, Consorzio Interuniversitario Nazionale per l'Informatica (organizzatore di Itasec con l'università Ca' Foscari di Venezia). Consideriamo infatti che Industry 4.0 significa, tra l'altro, tanta intelligenza in più nelle nostre fabbriche: sensori, robot, software.

Laddove ci sono software e connessioni ci possono essere vulnerabilità informatiche: si amplia di tanto la superficie d'attacco. Non preoccuparsi di difenderla in modo adeguato significa esporsi a rischi enormi. È un po' come se le repubbliche marinare del medioevo avessero potenziato le navi mercantili senza fare crescere di pari passo la flotta navale a protezione. Sarebbe stata una bella pacchia per i pirati. Informatici, nel nostro caso. Il mondo l'ha già capito: infatti, secondo Gartner, la spesa complessiva globale per la sicurezza in ambito Internet delle cose è stata di 348 milioni di dollari nel 2016, in crescita di circa il 24% rispetto al 2015.

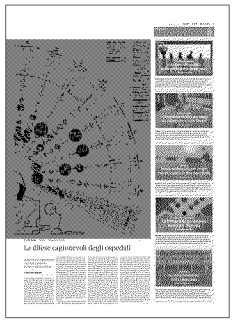
Per fortuna il piano Industry 4.0 non ignora del tutto il tema cyber security. Vi dedica un capitolo (sebbene senza risorse specifiche). «Indirettamente, Industry 4.0 aiuterà la cyber security nazionale perché incentiva anche gli investimenti in software, che possono essere quelli di sicurezza», dice Alvise Biffi, presidente Assolombarda e vice presidente Piccola Industria Confindustria e fondatore di Secure Networks. «La difficoltà sarà veicolare sui piani aziendali cybersecurity gli incentivi possibili con Industry 4.0, dato che la sicurezza non è solo una questione di nuovi software ma richiede anche cambi organizzativi e di processo, nuove competenze», aggiunge Biffi. Un ruolo in tal senso lo potranno svolgere le associazioni di settore e i competence center, previsti dal piano Industry 4.0 (anche se per ora con molte meno risorse di quelle annunciate dal Governo e con obiettivi poco definiti).

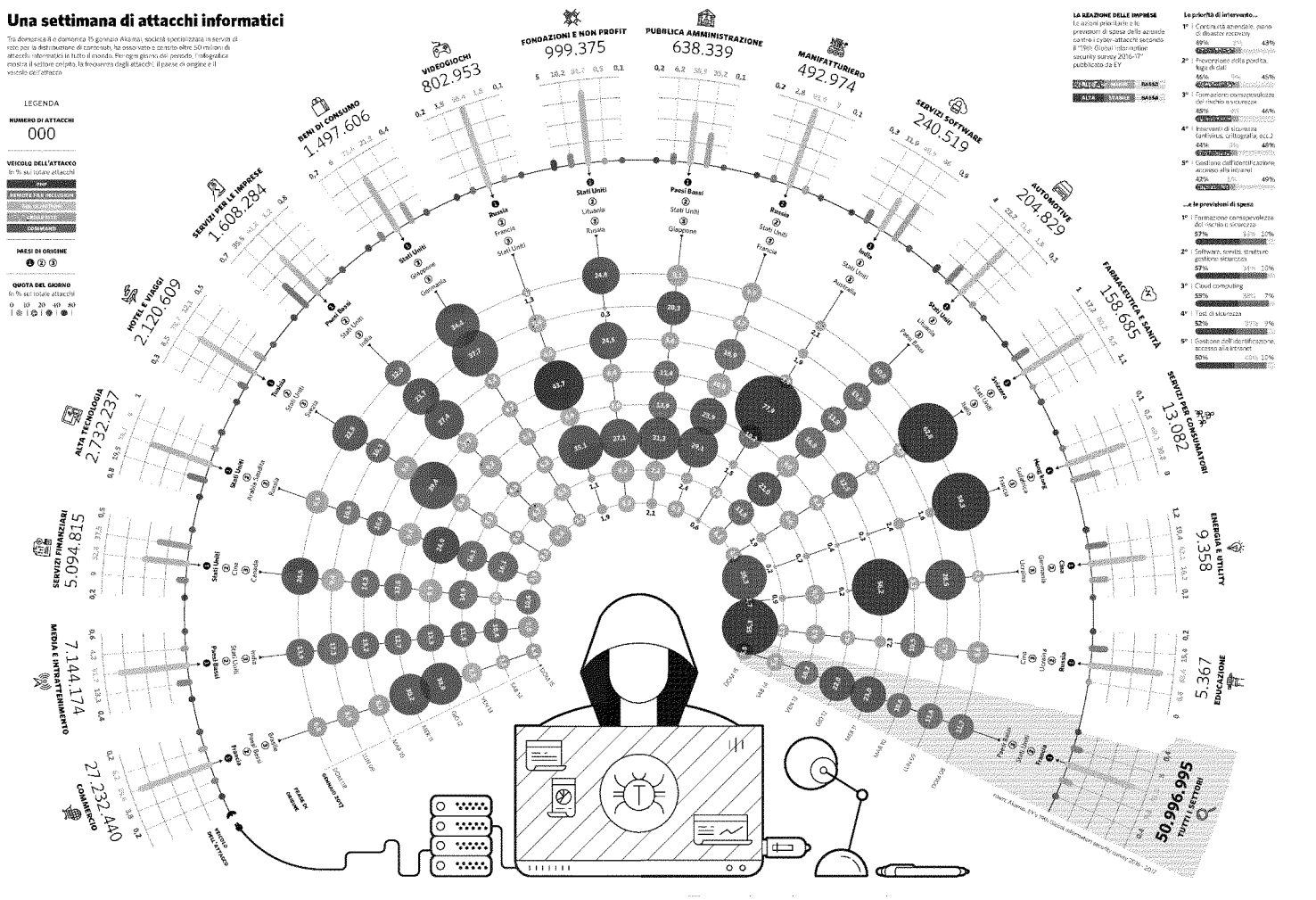
«In Confindustria stiamo sviluppando un modello che traduca il framework della cybersecurity nazionale (elaborato dal Cini) in azioni semplici, alla portata di tutte le aziende», dice Biffi. Sarà uno strumento gratuito in forma di modulo web, dove le aziende saranno guidate passo passo per capire il proprio livello di esposizione al rischio informatico e cosa fare per rimediare. «Sarà pronto per marzo. E sarà facile da usare, anche per le aziende meno tecnologiche», dice Biffi. «La sfida principale sarà aiutare le nostre tante Pmi, dove le competenze tecnologiche sono bassissime, a crescere in innovazione e sicurezza assieme, nei prossimi anni», conferma Presidente della Sezione Servizi Innovativi e Tecnologici di Confindustria Vicenza, che sta organizzando corsi specifici per Industry 4.0, sul territorio, con un modulo dedicato alla cybersicurezza.

«I nuovi pericoli informatici obbligano le aziende a fare un salto culturale: devono investire su tecnologie per la prevenzione del rischio; mentre finora si sono limitate a predisporre solo sistemi per reagire alle minacce che emergevano di volta in volta», ha detto a Itasec Mauro Palmigiani, country manager dell'azienda di sicurezza digitale Palo Alto Networks. Tra l'altro, da maggio 2018 si aggiunge anche la scure delle sanzioni (fino al 4% di fatturato) previste dal nuovo regolamento europeo privacy, se si subisce un accesso abusivo ai dati personali trattati dall'azienda. Avverte Prinetto: «Se le aziende investiranno in innovazione ma non in sicurezza potranno essere attaccate con facilità, certo; ma non solo: espongono a rischi anche i clienti che usano i loro prodotti. Ne deriva per le aziende un grosso danno di credibilità ed economico».

@AlessLongo

Si spaccia per "rinnovo abbonamento Whatsapp" la truffa che sfrutta vulnerabilità dei sistemi di sicurezza degli operatori per scalare 5 euro a settimana dal credito telefonico. Molte le vittime, anche tra gli esperti





L'urgenza di un ecosistema cyber nazionale

Il nostro paese non è pronto per affrontare attacchi sofisticati. Serve un piano

di **Roberto Baldoni**

Tutta l'economia di un paese sviluppato poggia sul cyberspace. I programmi di trasformazione digitale, irrinunciabili, come il piano industria 4.0 non faranno che aumentare questa dipendenza. Il cyberspace è la cosa più complessa e articolata che l'uomo abbia mai concepito, unione di migliaia di reti dati e di stratificazioni di software che interconnettono uomini e cose in giro per il mondo. Tuttavia, questa complessità, non avendo come fulcro la sicurezza, è generatrice di vulnerabilità nelle reti e nei programmi software e nelle loro interazioni. I cyber-criminali cercano di sfruttare queste vulnerabilità, molto spesso anche umane, per penetrare i nostri computer e trafugare dati o bloccare i nostri sistemi. La ricerca, i governi e l'industria studiano soluzioni per rendere sempre più difficile e costoso questo accesso indebito per l'attaccante. In questo gioco tra "guardia" e "ladri" la capacità di fare sistema tra le varie componenti di un paese è condizione primaria per una risposta efficace.

In Italia non siamo all'anno zero nella cybersecirity. Dopo il Dpcm Monti, che ha strutturato l'architettura cyber Nazionale, alcuni passi sono stati fatti, la sinergia sistemica tra ricerca e governo ne è un esempio. Troppo poco. I fatti di questi giorni mostrano che siamo impreparati ad affrontare attacchi con un minimo di sofisticatezza, non certo comparabili ad esempio a quelli portati da APT28, gli hacker russi che hanno attaccato Italia e Nato. In un mondo che corre, i governi dei paesi più industrializzati pongono la cybersecurity in cima alle proprie agende investendo imponenti risorse in programmi (almeno) quinquennali. Il nostro Paese si sta muovendo troppo lentamente e praticamente senza risorse.

Cosa fare. L'estate scorsa abbiamo atteso invano una rivisitazione del Dpcm Monti con l'attivazione di una "Unità di Missione" all'interno della Presidenza del Consiglio dei Ministri che prendesse in mano le redini del problema. Benché la nascita di una struttura che centralizzi competenze sia auspicabile, non sarà questa struttura da sola a risolvere il problema! Abbiamo bisogno di creare un "ecosistema cyber nazionale", composto da alcune organizzazioni di dimensioni adeguate, in termini di personale e competenze, inserite sia nel settore pubblico che in quello privato. Queste strutture devono abilitare una fitta rete di collaborazioni e devono essere in grado di impostare "operations" sia a livello internazionale che tra settore pubblico e settore privato nazionale. Squadra per la risposta ad emergenze informatiche, certificazione di dispositivi (hardware/software/firmware), ricerca, supporto alle industrie nazionali, cybercrime, cyber-intelligence e cyberwarfare sono esempi di aree che richiedono strutture da realizzare o da ampliare appropriatamente. Se l'Italia non sarà in grado, come altre nazioni, di far partire questi centri sarà sempre più tagliata fuori da operazioni internazionali riservate a una élite di nazioni "cyber-dotate" e regredirà sempre più come sistema paese.

L'ecosistema richiede di attivare un percorso virtuoso di trasferimento tecnologico tra università e impresa con un supporto strategico governativo, per consentire che le miriadi di prototipi, proof of concept, algoritmi innovativi che vengono elaborati dalla ricerca italiana, spesso lasciati in un cassetto, abbiano la possibilità di trasformarsi in opportunità di business. Inoltre nell'ecosistema si devono fare crescere e proteggere le startup che producono tecnologia di interesse strategico nazionale. In questo gli Stati Uniti e Israele sono esempi virtuosi, seppure diversi tra loro. Ci si potrebbe domandare: perché questo modello di trasferimento tecnologico dovrebbe attivarsi nella cybersecurity e non in altri settori dell'informatica? Perché la cybersecurity italiana è una comunità coesa nella quale tutti comprendono da tempo i rischi e la portata della minaccia e l'importanza della stretta collaborazione tra pubblico-privato-ricerca.

Competenze. Per implementare l'ecosistema abbiamo bisogno di competenze. Non ne abbiamo molte in Italia. Quindi, in una prima fase, dobbiamo concentrare le competenze. Parallelamente, dobbiamo crearne altre attraverso un programma specifico che recluti docenti universitari allo scopo di creare nuovi corsi di laurea sul territorio nazionale per aumentare la "workforce" agendo in sequenza anche sulle scuole di dottorato e sui licei.

La cybersecurity è un tema tecnico, benchè multidisciplinare, quindi c'è bisogno di ricercatori e ingegneri per trattarla in maniera adeguata e di persone con altri profili ma con anni d'esperienza nel settore. L'incompetenza metterebbe a rischio l'intero ecosistema. Abbiamo bisogno da parte del Governo di un piano forte per la cyber sicurezza nazionale, di investimenti e di un programma pluriennale con obiettivi precisi. È la condizione necessaria per rimanere agganciati al treno dei paesi sviluppati, senza che le nostre aziende e amministrazioni o i nostri cittadini rimangano ostaggi non di APT28, ma di un qualsiasi ragazzino "sufficientemente smart".

VENEZIA *Il team di Diego Piacentini, commissario all'Agenda Digitale a Palazzo Chigi, ha avviato il primo programma nazionale per facilitare la scoperta, la condivisione e la correzione di vulnerabilità informatiche nei sistemi delle Pubbliche amministrazioni. Da una prima stima, sembra che la maggior parte dei siti della Pa siano su un software non aggiornato dal 2005.*