G L /X Q H G u J L X J Q R

Sommario Rassegna Stampa

ItaliaOggi Sette

Settimanale Data 06-06-2022
Pagina II/III
Foglio 1 / 2

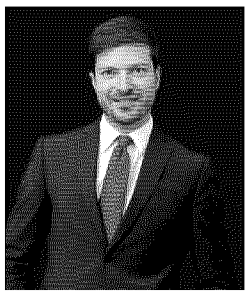
L'Italia è tra i primi 5 paesi del mondo con il maggior numero di aggressioni sulla rete

Cybersecurity, uno scudo contro gli attacchi alle imprese

PAGINE A CURA DI ALBERTO GRIFONE


Giulia Zappaterra


Stefano Mele


Vincenzo Colarocco


Massimiliano Masnada


Simona Lavagnini


Pierluigi Perri

La difesa degli asset informatici delle imprese e delle società che erogano servizi fondamentali (come nella sanità) è un problema di crescente rilevanza per il Paese. Secondo l'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano, a fronte di una crescita delle minacce (1053 incidenti gravi nel primo semestre del 2021, +15% rispetto al primo semestre 2020, dati Clusit), il 31% delle grandi imprese italiane rileva un ulteriore aumento degli attacchi informatici. Effetti riconducibili anche qui sia al nuovo modo di operare da remoto, causa Covid e, più di recente, alla guerra in corso in Ucraina.

Nei giorni scorsi il governo ha presentato il Governo Draghi la prima strategia 2022-2026 per la difesa del Paese contro gli attacchi di criminali e potenze straniere su internet, assegnando risorse pari all'1,2 per cento degli investimenti lordi del Paese, con possibili sgravi fiscali per le aziende che investono in cyber security. Gli studi legali vengono sempre più spesso coinvolti e consultati dalle aziende per sviluppare servizi e consulenze preventive.

«L'assistenza nella gestione di cyberattacchi richiede un team multidisciplinare. A tal fine abbiamo creato in Italia e a livello internazionale una gruppo dedicato alla cybersecurity con competenze in materia di privacy, Innovation Technology, litigation, assicurativo e penale per poter fornire al cliente un'assistenza a tutto tondo sia rispetto alla compliance cyber che rispetto alla risposte ad eventuali situazioni di attacco informatico», spiega **Giulia Zappaterra**, senior lawyer nel dipartimento Intellectual property & technology di **Dla Piper**. «L'incarico più rilevante degli ultimi 6 mesi in materia di cybersecurity riguarda l'assistenza ad un cliente in un cyberattacco di tipo *ransomware* che ha impattato oltre 40 giurisdizioni con la conseguente necessità di procedere alle relative notifiche alle diverse autorità locali e comunicazioni agli interessati, alla gestione delle indagini interne, dei rapporti con i *threat actor* e richieste delle autorità. Con il network di Dla Piper e delle nostre best friend law firm siamo stati in grado di gestire la questione in modo efficiente fornendo assistenza in tempo reale al cliente in un momento di grande difficoltà operativa». Guardando ai prossimi mesi «prevediamo una forte crescita nella compliance cyber. Su questo infatti l'attività sta aumentando esponenzialmente rispetto agli scorsi anni, in quanto le imprese stanno prendendo coscienza del fatto che è necessario non solo adottare sistemi idonei a proteggersi da eventuali attacchi ma è altrettanto necessario adottare delle policy interne che tutelino l'azienda dai comportamenti interni (ad esempio anche dei propri dipendenti) e dimostrare di aver fatto quanto necessario attraverso procedure valide e applicabili. Si passa quindi da un contesto di pura sicurezza tecnica a quello di sicurezza anche documentale, volto a dimostrare le proprie buone pratiche e la prontezza nel reagire ai rischi di cybersecurity».

Per **Stefano Mele**, partner esperto in Cybersecurity del dipartimento Proprietà Intellettuale, Tmt e Cybersecurity dello studio legale **Gianni & Origoni,** oltre a quelle legate all'attuazione del reticolato normativo previsto dal Perimetro di sicurezza nazionale cibernetica, «le principali problematiche che stiamo gestendo sono legate al filone del supporto strategico e legale in caso di attacchi cyber di tipo ransomware o di operazioni cibernetiche dirette ad un possibile sabotaggio dei sistemi informatici o allo spionaggio e alla sottrazione di informazioni. Inoltre, sempre più multinazionali nel settore tecnologico ci chiedono un supporto per valutare se i loro prodotti e servizi siamo o meno in linea con le normative europee e nazionali in materia di cybersecurity. Infine, se guardiamo alle attività un po' più «classiche» degli studi legali, c'è una richiesta sempre maggiore nelle operazioni di M&a di svolgere un'analisi legata anche al rischio cyber e, ovviamente, alla protezione dei dati personali». In ambito nazionale, insieme ai clienti, lo Studio guarda con interesse alle azioni che il governo italiano ha delineato all'interno del Piano nazionale ripresa resilienza (Pnrr) e i pilastri della ormai prossima nuova strategia nazionale in materia di sicurezza cibernetica, che inevitabilmente avranno numerose ricadute normative.

«A livello europeo siamo in attesa della cosiddetta «Direttiva Nis 2» (*Network and Information Security*), così come stiamo già analizzando le ricadute sul mercato dei nostri clienti del «Data Act» e della parte del «Cybersecurity Act» inerente alla creazione della prima certificazione europea sui livelli di cybersecurity dei prodotti, servizi e processi utilizzati all'interno dei confini dell'Ue. I continui e sostanziali interventi del legislatore europeo e nazionale nel settore della cybersecurity, che già oggi si delineano in maniera molto netta all'orizzonte, non potranno che far registrare un segno positivo nella crescita del mercato legale anche in questo 2022. Cosa che, peraltro, avviene in maniera costante dal 2018, ovvero a seguito dell'entrata in vigore della prima «Direttiva Nis». Mercato che, però, almeno a mio avviso, avrà una vera e propria esplosione dal 2023 in poi».

«Il team che si occupa delle problematiche della Cyber security è composto da tre professionisti esperti che forniscono consulenza a 360 gradi. In particolare, si occupano di fornire assistenza legale e tecnica già nella fase prodromica di progettazione ed implementazione degli asset informatici e supportano il cliente anche nell'eventuale e delicato momento conseguente ad un incidente informatico», spiega **Vincenzo Colarocco** responsabile del dipartimento privacy dello **Studio Previti**, fresco di nomina nella Commissione Protezione dati personali del Consiglio Nazionale Forense.

«L'attività di consulenza in ambito cyber, infatti, deve avere cura non solo di risolvere i problemi legati al concretizzarsi di un incidente informatico, ma soprattutto consigliare il cliente affinché svolga le proprie attività di business nel modo più sicuro possibile, adottando tutte le misure tecniche ed organizzative necessarie ed idonee a limitare enormemente il rischio per la sicurezza informatica».

Negli ultimi mesi lo studio ha assistito ad una evoluzione delle tecniche di *phishing* – tecniche informatiche fraudolente che, tramite l'invio di comunicazioni apparentemente affidabili, consentono di rubare informazioni personali delle vittime quali dati di accesso, indirizzi email, numeri della carta di credito. «I criminali informatici hanno sviluppato sistemi più evoluti di sfruttando altri strumenti di comunicazione quali Sms (il c.d. *Smishing*) e chiamate vocali (*Vishing*).

Quest'ultima modalità risulta particolarmente efficace in quanto la comunicazione vocale telefonica porta ad un coinvolgimento maggiore della vittima. Altri vettori recenti e particolarmente efficaci sono i Social Network e le piattaforme di Instant Message (oltre 2 miliardi di utenti attivi al mese) oppure le campagne pubblicitarie targhettizzate. In particolare, a seguito di un attacco di smishing, che aveva portato alla sottrazione di importanti somme di denaro, siamo intervenuti tempestivamente e grazie all'intervento delle forze dell'ordine la banda di hacker è stata arrestata e le somme connesse al reato sono state sequestrate» conclude.

Altro studio molto attivo è **Hogan Lovells.** «I nostri clienti ci coinvolgono sia nella fase patologica, quanto cioè un incidente è avvenuto e devono effettuare valutazioni di rischio e avviare

159329

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

ItaliaOggi Sette

Settimanale Data 06-06-2022
Pagina II/III
Foglio 2 / 2

Studi in soccorso per aiutare le aziende a proteggere i dati

processi di notifica, sia nella fase fisiologica, cioè nella preparazione delle procedure interne di adeguamento alla normativa e di incident response», spiega **Massimiliano Masnada**, partner Hogan Lovells. «Abbiamo notato, inoltre, che la cybersecurity sta assumendo un ruolo di grande importanza anche in fase di negoziazione di contratti.

A parte le disposizioni del Gdpr sul data breach, sicuramente uno dei passaggi normativi più attesi è la Nuova direttiva Nis 2, attualmente in discussione, che dovrebbe allargare l'ambito applicativo dell'attuale Nis e apportare delle innovazioni interessanti, soprattutto affrontando il tema della sicurezza della supply chain e prevedendo un enforcement più stringente.

«Sempre a livello di Unione Europa, è bene ricordare che è in discussione anche la direttiva sulla *Digital operational resilience for the financial sector*. In ambito nazionale invece, siamo in attesa del completamento del processo che ha portato alla creazione dell'Agenzia Nazionale per la Cybersicurezza e ci aspettiamo un aggiornamento della disciplina in materia di sicurezza e incidenti nel settore delle telecomunicazioni, anche alla luce dell'entrata in vigore del nuovo codice delle comunicazioni elettroniche» aggiunge.

Le aziende sono molto preoccupate di proteggere i sistemi aziendali, dal punto di vista della compliance cui sono tenuti, a vari livelli, come anche per proteggere le loro informazioni riservate e i loro asset. «La clientela può essere adeguatamente preparata dal punto di vista tecnico e informatico, ma spesso non ha in essere adeguate protezioni anche di tipo giuridico, soprattutto contrattuale, per controllare al meglio le procedure interne e per minimizzare i rischi che potrebbero presentarsi attraverso violazioni da parte di dipendenti, collaboratori o fornitori, nei confronti dei quali si è generalmente più esposti.

Per questa ragione è spesso necessario integrare il livello di protezione tecnico con un adeguato sistema di policy interne e di contratti, oltre che con un training costante (tecnico e legale) dello staff del cliente» dice **Simona Lavagnini**, founding partner di **Lgv Avvocati**. «Si tratta di un ambito dinamico che è in continua evoluzione. A nostro modo di vedere un tema che ci pare cruciale è quello toccato dalle normative in materia di protezione dei dati personali, dell'intelligenza artificiale, nonché di servizi digitali in senso ampio.

Maria Livia Rizzo

Fabrizio Tarocco

Marta Minonne

Fra le iniziative legislative più importanti, da tenere in considerazione anche per i riflessi sulla cybersecurity, ci sono la proposta europea di regolamento sull'intelligenza artificiale e il Digital Service Act. Il settore è in forte crescita, sia per quanto riguarda la consulenza preventiva per fare in modo che i sistemi informatici interni delle aziende siano sufficientemente protetti, sia per quanto riguarda le azioni nel caso di violazione dei sistemi. La consulenza deve essere costante, dinamiche e interdisciplinare, oltre che tenere conto di aspetti di internazionalità (essendo spesso i temi crossborder). Per quanto riguarda invece la litigation, è cruciale partire da una buona base di descrizione tecnica dell'evento, che può derivare da sistemi di rilevazione ove inseriti a monte nelle strutture informatiche, ovvero anche tramite investigazioni ex post, che possono essere attuate attraverso esperti in analisi complessa dei sistemi informatici e del traffico di rete. Importante è anche affiancare le strategie di protezione, combinando a seconda delle esigenze del caso strumenti di difesa civile con strategie di tipo penale» chiosa.

Tavella Studio di Avvocati ha costituito un dipartimento data protection e cyber security coordinato da **Pierluigi Perri** of counsel, professore di Sicurezza informatica, privacy e protezione dei dati sensibili presso l'Univerisità degli Studi di Milano. In più, il team vede due risorse interne che hanno seguito un percorso di formazione specifico nel diritto IT e nella protezione dei dati. «Le principali operazioni che abbiamo seguito riguardavano la gestione di incidenti informatici sui sistemi dei clienti dovuti sia ad attacchi esterni dolosi che avevano compromesso la funzionalità del sistema e la disponibilità dei dati, sia ad azioni colpose svolte da personale interno o comunque da personale che aveva un accesso alle risorse informatiche dell'azienda», spiega Perri.

«È evidente che un attacco informatico genera una situazione di crisi che deve essere gestita, anche nell'ottica della tutela della reputazione dell'impresa. Possiamo distinguere due situazioni: una situazione di crisi e una di preparazione a possibili eventi indesiderati. Nella situazione di crisi, le principali richieste riguardano la corretta gestione della fase post-attacco, che riguarda soprattutto la presentazione di eventuali denunce, le operazioni di controllo del danno e tutela della proprietà intellettuale dell'azienda e dei dati dei clienti, nonché il rafforzamento del sistema sulla base dell'esperienza maturata a seguito dell'attacco. Nella fase di preparazione rispetto a possibili incidenti informatici, ci si concentra sulle operazioni di audit del sistema e di redazione e formazione dei dipendenti sulle policy aziendali. È risaputo che il fattore umano rappresenta spesso l'elemento più debole della cyber security».

«Come da trend generale, la maggior parte delle operazioni seguite dal nostro studio ha riguardato analisi del livello di rischio di data breach legati ad attacchi informatici commessi tramite phishing o utilizzando malware di tipo ransomware cryptolocker», dice **Maria Livia Rizzo** dello **Studio Stefanelli&Stefanelli**. «Un caso particolare ha riguardato l'attacco a un indirizzo e-mail effettuato tramite una modifica delle impostazioni del relativo account, che inoltrava in automatico qualunque risposta alle mail che partivano da quell'indirizzo (contenenti liste operatorie) a un indirizzo mail terzo. Non mancano, ad ogni modo, clienti che in ottica di prevenzione ci chiedono un supporto specifico per individuare le misure di sicurezza, non solo tecniche ma anche organizzative, più idonee a contrastare le minacce IT». Il legislatore è particolarmente consapevole del fatto che, per rendere efficace la digitalizzazione, non è più possibile separare il concetto di tecnologia da quello di cyber security.

«Questo aspetto è reso evidente dall'incremento di norme volte a migliorare gli standard di sicurezza informatica che negli ultimi anni si sono susseguite sia a livello europeo che nazionale. Il prossimo passaggio normativo atteso riguarda le aziende che svolgono un ruolo chiave nella fornitura di servizi essenziali all'interno dell'Unione europea, o che operano in settori critici come quello dell'healthcare, ed è rappresentato dalla Direttiva Nis II, la cui proposta è stata pubblicata il 4 novembre 2021, e che andrà a sostituire la Direttiva Nis 1148/2016, recepita in Italia dal Decreto Nis del 2018. Dato il ruolo di primo piano svolto dal settore digitale nell'economia globale, un focus sulla sicurezza, resilienza e affidabilità dei sistemi Information Technology sarà necessariamente al centro delle strategie aziendali del prossimo futuro. Predisporre modalità di salvaguardia dei sistemi informatici e di protezione dei dati digitali diventerà sempre più importante» conclude.

Weigmann Studio Legale, grazie alla significativa esperienza, per il tramite di un team dedicato composto da **Fabrizio Tarocco**, equity partner e **Alessio Chiabotto**, Associate, offre servizi di consulenza ed assistenza legale tanto alle imprese che abbiano specifiche necessità in materia, quanto ai tecnici/esperti di compliance per coadiuvarli nel loro ruolo. «Registriamo un crescente interesse da parte delle imprese e, conseguentemente, un significativo incremento delle richieste di consulenza, sugli aspetti connessi all'emersione ed applicazione delle più recenti tecnologie al settore della sicurezza informatica, ad esempio valutazioni di compliance, rispetto alla legislazione in materia di protezione dei dati personali e di diritti di proprietà intellettuale, di sistemi di machine learning utilizzati con finalità di threat intelligence, consulenza su sistemi innovativi volti garantire l'integrità dei dati e a consentire la verifica delle identità digitali, consulenza su sistemi di mitigazione dei problemi di sicurezza attraverso sistemi automatizzati di analisi automatizzata del codice e consulenza sui sistemi di prevenzione in ambito aziendale dall'utilizzo da parte di dipendenti e collaboratori di prodotti software o contenuti digitali in violazione dei corrispondenti diritti d'autore di terzi».

«Siamo soliti assistere i nostri clienti nell'ambito dell'intero processo di adeguamento alla normativa privacy. Ci viene spesso richiesto supporto nella revisione e implementazione di misure tecniche e organizzative, nella gestione degli incidenti, nonché assistenza nella predisposizione di valutazioni di impatto per attività di trattamento che richiedono l'uso di nuove tecnologie. Seguiamo inoltre i nostri clienti nella redazione di policy, tra cui la documentazione di eventuali data breach e la predisposizione di linee guida sulla conservazione dei dati e sull'uso di strumenti informatici» spiega **Marta Minonne** di **Orsingher Ortu Avvocati Associati.**

Nell'ambito della strategia per il mercato unico digitale elaborata dalla Commissione Europea, vi è certamente l'entrata in vigore del nuovo Regolamento ePrivacy, che mira ad accrescere la fiducia nei servizi digitali e nella sicurezza degli stessi. «Di particolare interesse è anche la proposta per un Regolamento europeo volto a stabilire regole armonizzate in materia di intelligenza artificiale. Si tratta, infatti, di un settore tecnologico in grande espansione negli ultimi anni che, se da un lato consente di ottenere benefici economici e sociali per le aziende, dall'altro porta con sé rischi connessi all'uso di tali tecnologie e possibili impatti negativi per gli individui.

È prevedibile che nel corso dell'anno si verifichi un incremento di incidenti e attacchi informatici con l'uso di nuovi e sempre più insidiosi malware, nonché di sofisticati sistemi di phishing. Essendo ormai confermato il trend che vede un numero crescente di aziende avvicinarsi al mondo dell'online e indirizzare verso tale settore le proprie attività lavorative, ci si aspetta un accrescimento degli investimenti sulle misure tecniche e organizzative volte a prevenire possibili attacchi e incidenti informatici» chiosa.

© Riproduzione riservata

Supplemento a cura
di Roberto Miliacca
rmiliacca@italiaoggi.it
e Gianni Macheda
gmacheda@italiaoggi.it

159329

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

ItaliaOggi Sette

Settimanale Data 06-06-2022
Pagina 5
Foglio 1 / 2

L'allarme arriva dal rapporto di The European House – Ambrosetti: scarsi gli investimenti

La ricerca non cambia in valore

Italia in testa per qualità e in coda per capacità di innovare

Pagina a cura
DI ANTONIO LONGO

L'Italia si conferma un'eccellenza per la qualità della ricerca accademica, con 1.594 citazioni ogni 100 ricercatori, ma si rivela critica la capacità di tradurre tale eccellenza scientifica in innovazione e valore economico e industriale. Ad attestarlo sono i contenuti del rapporto «*Super Smart Society: verso un futuro più sostenibile, resiliente e umano centrico*», realizzato dalla Innotech Community di **The European House – Ambrosetti**. Secondo l'Ambrosetti Innosystem Index, l'Italia è, infatti, quintultima per capacità d'innovazione, ma prima nella qualità della ricerca scientifica, su 22 paesi analizzati. Il report si basa sull'aggiornamento dell'Ambrosetti Innosystem Index che considera l'ultimo triennio di dati disponibili 2018-2020 e classifica la performance complessiva dell'innovazione di 22 paesi «modello» mediante l'analisi di 14 indicatori chiave.

«Dal rapporto emerge un'Italia con alcuni importanti punti di forza, come la bioeconomia e la capacità dei nostri ricercatori di produrre eccellenza scientifica, ma allo stesso tempo frenata e con grandi opportunità da cogliere per quanto riguarda la capacità di costruire un solido ecosistema dell'innovazione, condizione essenziale per accelerare il cammino verso lo sviluppo sostenibile e la Super Smart Society», spiega **Valerio De Molli**, managing partner & ceo di The European House - Ambrosetti. «Per fornire una bussola per la business community e i policy maker e guidare le future scelte strategiche del paese in ambito innovazione, nel rapporto avanziamo quattro proposte programmatiche». Secondo gli analisti, quindi, le risorse del Pnrr devono indirizzarsi verso progetti in grado di massimizzare il potenziale di innovazione; occorre creare un meccanismo virtuoso per tradurre il primato di ricerca scientifica in innovazione concreta; bisogna promuovere riforme a sostegno dell'imprenditorialità innovativa; serve lanciare un new deal delle competenze per preparare i cittadini e le aziende italiane di oggi e di domani a prosperare in una società digitale e sostenibile.

Promossi e bocciati. Secondo l'Ambrosetti Innosystem Index, nell'ecosistema dell'innovazione l'Italia si trova nelle retrovie, posizionandosi in quintultima posizione. Al primo posto gli Stati Uniti (con un punteggio di 5,1), al secondo posto si piazzano Israele, Germania e Austria (4,6). Per quanto riguarda, invece, gli investimenti in ricerca e sviluppo, la Germania vanta il primato in Europa con 105,9 miliardi di euro investiti, più di quattro volte gli investimenti dell'Italia, che si ferma a 25,4 miliardi di euro. Considerando il contesto mondiale, e rapportando gli investimenti in ricerca e sviluppo al pil, l'Italia si posiziona al di sotto della media Ue a 27 (2,2%) con l'1,5% del pil destinato alla ricerca. A fronte di tale scenario a tinte sbiadite, l'Italia si distingue, invece, per l'efficienza e la qualità della ricerca accademica anche se non si riesce a tradurre tale eccellenza in valore economico, anche in materia di registrazione di brevetti (19° posto). Dati negativi anche per quanto riguarda il tasso di mobilità netta degli studenti, rispetto al quale si posiziona come ultimo paese con un saldo netto positivo tra studenti in entrata e studenti in uscita. E ancora, il report considera il numero di start-up rapportato per milione di abitanti: a livello Ue si registra il primato dell'Estonia con 865 start-up/milione di abitanti, mentre l'Italia si attesta nella seconda metà della classifica con 234 start-up/milione abitanti. Si tratta, comunque, di un valore superiore alla media dell'Ue (190 start-up/milione di abitanti). In tale contesto, alla data del 31 dicembre scorso, l'Italia contava 14.077 start-up innovative iscritte al registro delle imprese, la maggior parte delle quali (75,7%) operante nei servizi alle imprese. I due poli più importanti si confermano Roma e Milano, dove sono localizzate, rispettivamente, il 18,7% e il 10,9% delle start-up.

Le nuove sfide. A giudizio degli esperti, l'Italia deve accelerare sull'innovazione per sviluppare nei prossimi anni una società sostenibile, resiliente e umano centrica. Sfruttando le opportunità che derivano, soprattutto, dal metaverso, dalla bioeconomia circolare, passando per la digitalizzazione della p.a., dalla decarbonizzazione e dalla transizione ecologica.

Nello specifico, gli analisti indicano nell'impatto del metaverso uno di fattori trainanti che possono guidare la crescita, aprendo mondi e possibilità impensabili fino a pochi anni fa. Oltre a settori come gaming e intrattenimento, infatti, non mancheranno spazi di utilizzo in ambito fashion, sanitario, retail, manifatturiero e nell'istruzione. Il rapporto stima che il numero di visori commercializzati ogni anno abbia già sorpassato le 5 milioni di unità annue e, con lo scoppio della pandemia, abbia subito una forte accelerazione, così nel 2022 sfiorerà le 15 milioni di unità vendute ogni anno.

Anche l'utilizzo di tecnologie di automazione e l'impiego dei robot si estendono ormai su vari ambiti, relativi sia al contesto industriale che alla vita quotidiana dei cittadini. Un mercato in forte crescita che nel 2021 ha prodotto 435 mila nuove unità che raggiungeranno, nel 2024, quota 518 mila. L'adozione di robot nei processi produttivi è interconnessa anche al tema legato al progressivo invecchiamento della popolazione che sta causando squilibri tra domanda e offerta di lavoro: l'automazione rappresenta una potenziale soluzione, consentendo alle aziende di mantenere invariata la propria produttività. Per esempio, la robotica riveste un ruolo rilevante nel settore automobilistico, con l'84% degli attori che si affida alle nuove tecnologie, e nel settore healthcare con il 57% dei business globali che ha implementato soluzioni robotiche, in grado di apportare benefici in termini di sicurezza, produttività e qualità del lavoro. Inoltre, per raggiungere gli obiettivi posti dall'Unione europea in termini di decarbonizzazione, sarà fondamentale intervenire sul settore dei trasporti. Nel 1990 rappresentava il 14% delle emissioni totali, mentre nel 2019 il 25%. L'Italia, secondo paese europeo per tasso di motorizzazione, dovrà intervenire, soprattutto, sul fronte delle auto private e fondamentali saranno i fondi destinati dal Pnrr, pari a 34 miliardi di euro, che serviranno a promuovere la conversione elettrica del trasporto pubblico e privato, lo sviluppo del trasporto rapido di massa e la digitalizzazione della logistica. Il report pone l'accento anche sulle nuove tecnologie per la decarbonizzazione, ossia il processo di riduzione del rapporto carbonio-idrogeno delle fonti energetiche. Sarà fondamentale il contributo del digitale al processo di decarbonizzazione, nel 2050 tra i settori in cui si prevede il più alto risparmio di Co2 grazie all'adozione di tecnologie digitali figurano trasporti (-22,8%), produzione di energia elettrica (-13,4%) e processi industriali (-8,6%). Gli esperti evidenziano, inoltre, che la crisi associata alla pandemia ha sottolineato la rilevanza della bioeconomia che ha registrato una contrazione della produzione meno marcata rispetto al totale dell'economia. In tale scenario, in Italia, nel 2020, il settore ha generato un fatturato pari a 317 miliardi di euro, pari al 10,2% del pil, e ha assorbito forza lavoro per circa 2 milioni di unità, pari al 7,9% del totale.

E ancora: l'Italia è prima in Europa per indice complessivo di circolarità e si conferma eccellenza e punto di riferimento, a livello mondiale, per la ricerca scientifica nell'ambito della bioeconomia. Infine, nel rapporto si ribadisce che l'esigenza di digitalizzazione è ormai imprescindibile

159329

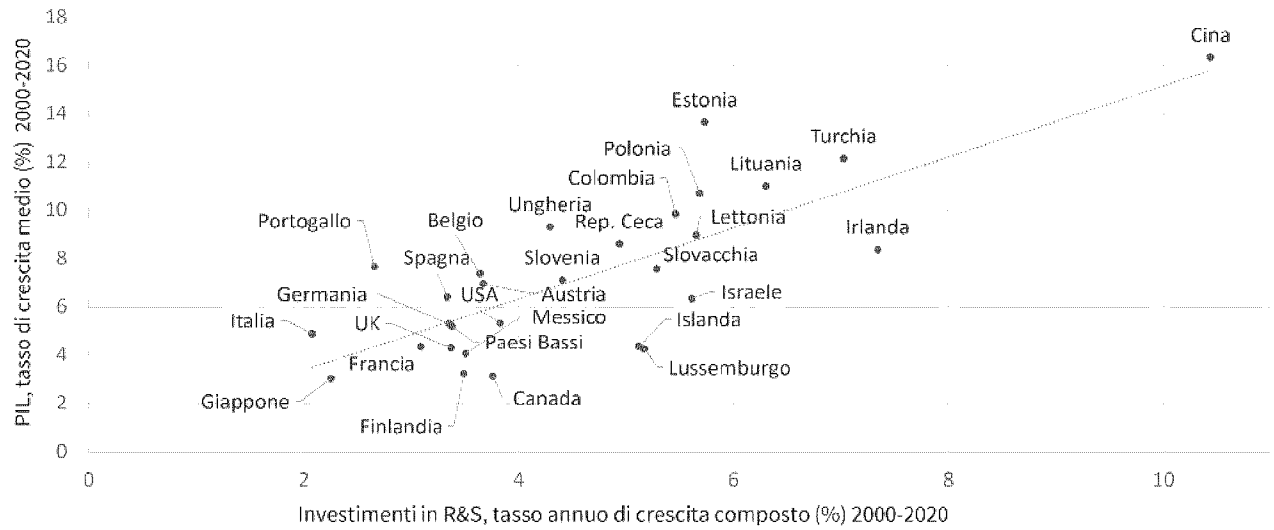
Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

per la p.a., nell'ottica di migliorare l'accesso a beni e servizi a cittadini e imprese. Nel 2021, la performance dell'Italia si è confermata al di sotto della media europea, nonostante i miglioramenti registrati negli ultimi anni. Secondo il Desi (Digital economy and society index), il livello di servizi pubblici digitali pone il paese al 18° posto. L'Italia ottiene, invece, risultati migliori rispetto alla media europea per quanto riguarda l'offerta di servizi pubblici digitali per le imprese e per la disponibilità di open data.

© Riproduzione riservata

Il rapporto ricerca-Pil

Relazione tra investimenti in R&S e crescita del PIL in 22 economie mondiali, 2000-2020



Fonte: elaborazione The European House - Ambrosetti su dati IMF e OECD, 2022


La ricerca non cambia in valore
Italia in testa per qualità e in coda per capacità di innovare

159329

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

Il Sole 24 ORE

Quotidiano Data 06-06-2022
Pagina 1
Foglio 1 / 3

AGEVOLAZIONI CASA

Superbonus, i casi ancora irrisolti dal bilancio agli inquilini delle Srl

Giorgio Gavelli —*a pag. 21*

Superbonus, i casi irrisolti dagli inquilini delle società al trattamento in bilancio

Agevolazioni

A due anni dal debutto nonostante quattro circolari restano ancora molti nodi

Spesso le risposte arrivano dopo che molti contribuenti hanno fatto scelte opposte

Pagina a cura di
Giorgio Gavelli

Nonostante quattro corpose circolari (24/E e 30/E del 2020, 16/E/2021 e 19/E/2022) e un numero impressionante di risposte a interpello, diversi aspetti sull'applicazione del superbonus restano ancora nel limbo. A due anni di distanza dal varo del decreto Rilancio (Dl 34/2020) chi si approccia alla materia deve spesso fare i conti su questioni di incerta interpretazione, al punto che i precetti del comma 5-bis dell'articolo 119 (irrilevanza delle violazioni meramente formali e limitazione di quelle rilevanti al singolo intervento irregolare) – apparsi ai più come pleonastici in quanto espressione di principi generali – saranno da tenere ben presenti quando inizieranno i controlli.

Senza avere l'ambizione di esaurire le tematiche dubbio, si possono sollevare qui le più frequenti (si veda anche la scheda).

Immobili locati da imprese

Nelle scorse settimane l'Agenzia ha affrontato una tematica per lungo tempo sommersa, anche se si conosceva una risposta della Dre Toscana (prot. 911-846/2021), peraltro ora in parte smentita dai recenti interpelli.

Il caso esaminato è quello in cui l'immobile è di proprietà di un soggetto non compreso nell'agevolazione (una impresa individuale o una società), ma si verifica la concessione in uso (locazione o comodato) a un soggetto "meritevole" ammesso all'agevolazione (persona fisica). Diversamente dalla Dre Toscana, le Entrate (risposte 288/2022 e 307/2022) non affermano che ogni volta in cui l'immobile appartiene all'impresa il 110% va negato, ma si inerpicano in una interpretazione casistica alquanto difficoltosa, soprattutto se confrontata con il dato letterale delle norme. Pare di capire che:

- in linea di principio andrebbe valorizzato l'utilizzatore dell'immobile, non il proprietario dello stesso;
- tale principio, tuttavia, diverrebbe inefficace qualora l'edificio «composto da più unità immobiliari» sia «interamente di proprietà o in comproprietà di soggetti» non agevolabili, come, appunto, le imprese, a meno che l'unità utilizzata dalla persona fisica non abbia accesso autonomo e sia funzionalmente indipendente;
- in ogni caso, senza alcuna spiegazione, si introduce una preclusione al bonus per tutti i soci di società commerciale che utilizzano (anche con contratto registrato di locazione o comodato) l'unità immobiliare residenziale di proprietà della società.

La sensazione è che l'interpretazione non sia (come dovrebbe) il risultato di una riflessione sul dato normativo, ma discenda direttamente da "come si vorrebbe" funzionasse l'agevolazione. Elemento che ha ben poco a che fare con l'aspetto giuridico e che, presumibilmente, in sede di contenzioso non incontrerà molto successo. Senza considerare che sapere ora che una agevolazione in vigore dal 1° luglio 2020 incontra limiti tanto ambigui crea conseguenze non di poco rilievo.

Il trattamento contabile

Altra questione di estrema rilevanza, spesso a torto dimenticata, è la fiscalità di questi bonus nell'ambito del reddito d'impresa, dopo che l'Oic (agli inizi di agosto 2021) ha reso definitivo il proprio documento in cui, in estrema sintesi, la detrazione viene assimilata a un contributo in conto impianti.

Nonostante l'Oic sia stato chiamato in causa dalla stessa Agenzia, non si conoscono documenti di prassi in cui sia dia seguito, a livello fiscale, alle modalità di contabilizzazione che sono state prescritte, del tutto innovative rispetto al passato. L'interpretazione prevalente (resa anche di recente nel corso del webinar organizzato dal Cndcec lo scorso 17 maggio) sostiene – facendo trasparire una sorta di "rassegnazione" – che questi bonus finiscano per creare materia imponibile, sotto forma di proventi o minori ammortamenti, per una combinazione "sfortunata" tra derivazione dal bilancio e assenza di una norma che disattivi questa conseguenza. Tra l'altro è una lettura che riguarda tutti i bonus casa, non solo il 110%, con pesanti ricadute sul passato.

159329

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

Non mancano di certo argomenti che porterebbero in altra direzione (si veda Il Sole 24 Ore del 20 agosto 2021, del 28 settembre 2021 e del 30 settembre 2021). Del resto la "derivazione" mal si adatta alle imprese minori, semplificati, minimi e forfettari compresi. Ma quello che qui si vuole sottolineare è che i bilanci 2021 sono stati chiusi (e le imposte calcolate) senza una "bussola" che guidasse il trattamento di voci di conto economico (non solo i bonus, ma anche i differenziali di acquisto e cessione) che, per molte imprese, rappresentano importi assai significativi.

Ricadute reddituali per i privati

Per i "privati", se nessuno – fortunatamente – si pone il tema dell'imponibilità (e sono sterilizzate anche le plusvalenze: risposta ad interpello 204/2021), non è banale il tema del trattamento dei differenziali positivi per quei soggetti che hanno acquistato i crediti d'imposta per utilizzarli in proprio o rivenderli. La norma da interpretare, nel caso specifico, parrebbe la lettera c-quinquies) del comma 1 dell'articolo 67 del Tuir, non certo di frequente applicazione.

© RIPRODUZIONE RISERVATA

I punti controversi

Alcune delle principali perplessità che ancora riguardano i bonus edilizi e la loro circolazione

1

SOGGETTI

Applicazione del superbonus in caso di proprietario impresa con immobile concesso in uso a persona fisica.

- Le recenti risposte ad interpello 288/2022 e 307/2022 hanno riacceso il dibattito su queste fattispecie, in cui l'interpretazione dell'Agenzia è piuttosto "ce rvellotica" e non sorretta dal dato normativo: secondo il Fisco, quando l'immobile è posseduto interamente da un'impresa, l'inquilino persona fisica non ha diritto al superbonus. Inoltre, sempre escluso il socio utilizzatore.

Soggetti del terzo settore: Odv, Aps, Runts.

- Per gli enti del Terzo settore l'articolo 119 del Dl 34/2020 richiama una legislazione oramai superata dall'avvento del Runts: manca una tabella di raccordo chiara.

2

FISCALITÀ

Conseguenze reddituali dei bonus.

- L'Agenzia non ha mai dato seguito al documento Oic sulla contabilizzazione dei bonus, nonostante l'avesse richiesto lei stessa.

La disciplina è quindi avvolta nella nebbia.

- Non sono mai stati chiariti, inoltre, gli aspetti riguardanti l'interposizione dei soggetti privi di partita Iva nella circolazione dei bonus.

3

VISTO DI CONFORMITÀ

Congruità della spesa e competenza.

- Non è ancora chiaro se il compenso per il visto di conformità debba essere dichiarato "congruo" e come dimostrarlo. Le Faq dell'Enea datate 12 aprile e relative al Dm Mite lascerebbero intendere di no.
- Per le imprese va chiarito se la spesa relativa al visto di conformità si imputa secondo il criterio di competenza (tendenzialmente in base al momento di ultimazione dei lavori).
- Va sciolto anche il nodo del visto 2022 su un bonus facciate con spese per i lavori sostenuti nel 2021, chiarendo se la detraibilità è al 90% (come i lavori) o al 60% (secondo il criterio di imputazione temporale della spesa, come pare logico).

4

SAL PER LE VILLETTE

Raggiungimento della soglia di lavori realizzati utile per poter proseguire sino al 31 dicembre con il 110% nelle "villette".

- Mistero su chi e come debba "asseverare" il raggiungimento del risultato del 30% di lavori alla data del 30 settembre.

5

LIMITI DI SPESA

Compatibilità in presenza di interventi complessi.

- Molti interpelli riguardano il cumulo tra i limiti previsti specificatamente dagli articoli 119 e 119-ter del Dl 34/2020 ed il limite del bonus casa di 96.000 euro (articolo 16-bis del Tuir).
- Molto complesso anche declinare il limite di spesa "condominiale" (o del piccolo edificio con unico proprietario) per i lavori alle parti comuni con quello delle singole unità, in particolare nel caso di demolizione e ricostruzione.
- Per i soggetti del Terzo settore è previsto un limite di spesa maggiorato dal comma 10-bis dell'articolo 119, legato a casistiche, condizioni e metodi di calcolo della superficie che non sono mai stati oggetto di istruzioni, con forti difficoltà di applicazione.

6

BIFAMILIARI

Due villette di proprietari diversi con parti comuni.

- Nella pratica – in presenza di condominio minimo come una villetta bifamiliare – i comportamenti dei contribuenti sono assai disomogenei: titolo edilizio, fatturazione, approccio ai bonus seguono spesso percorsi diversi. Probabilmente per la scarsa chiarezza delle risposte.

7

COMUNICAZIONE E OPZIONI

I termini per il 2022 e la correzione degli errori.

- Non è chiaro il perimetro dei soggetti ammessi all'invio della comunicazione entro il 15 ottobre. Tutto fermo anche sulla regolarizzazione degli errori dopo il quinto giorno del mese successivo all'invio.

© RIPRODUZIONE RISERVATA

159329

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.