

Gdpr e cyber security, le startup italiane dormono: ecco tutte le opportunità perse

LINK: <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-e-cyber-security-le-startup-italiane-dormono-ecco-tutte-le-opportunita-perse/>

Gdpr e cyber security, le startup italiane dormono: ecco tutte le opportunità perse Home Sicurezza digitale Privacy Condividi questo articolo A un anno dalla piena operatività del Gdpr, a un'analisi risulta che le startup italiane non abbiano saputo coglierne le opportunità di business e non siano riuscite a creare la necessaria integrazione tra settore legaltech e mondo cybersecurity. Vediamo perché, quali sono i trend di mercato e cosa serve per una svolta 1 minuto fa Giuseppe Vaciago Partner **R&P Legal** e fondatore di Tech&Law Center A una prima analisi, il mercato delle startup italiane ha perso tutte le buone opportunità di business sorte dopo l'entrata in vigore del GDPR. In particolare, per creare soluzioni integrate in grado di far dialogare in modo armonico ed efficiente il settore IT con la funzione 'legal', 'compliance' e 'internal audit' delle aziende più strutturate. Poche società, infatti, hanno colto tale collegamento sia a livello di comunicazione che di soluzioni software. Un'altra sfida che, a livello nazionale, si sta rischiando

di perdere è quella del settore **legal**-tech. Negli ultimi anni a livello mondiale il mercato delle **legal**-tech è cresciuto esponenzialmente. Il totale degli investimenti è stato tra il 2012 e il 2017 di 2,15 miliardi di dollari. La sproporzione tra Stati Uniti e resto del mondo è netta: negli Stati Uniti sono stati investiti 2 miliardi di dollari, in Europa 93 milioni di dollari, mentre in Canada 30 milioni. Interessante notare, invece, che nel solo stato di Israele l'investimento è stato pari a 12 milioni. A livello italiano, il settore del **legal**-tech è ancora praticamente inesistente: ad oggi vi sono solo 13 società iscritte nel registro delle startup innovative della Camera di Commercio, a differenza del Regno Unito dove sono già 59. È, in ogni caso, evidente che il mercato europeo non ha ancora recepito le potenzialità di questi servizi a differenza di quello americano, dove il sistema giuridico (common law) e le maggiori potenzialità economiche del settore **legale** hanno permesso una crescita più repentina. Per arrivare ad una prima conclusione, solo una corretta sintesi tra il

settore **legal**-tech e il mondo della cybersecurity può essere in grado di essere di fornire soluzioni conformi a livello normativo e in linea con gli standard di sicurezza che saranno richiesti dopo l'entrata in vigore del Cybersecurity Act. Indice degli argomenti Cybersecurity startup: il panorama nazionale e internazionale a confronto Il mercato della cyber security I principali trend di mercato Gdpr e startup Il mondo delle startup in Italia Cybersecurity startup: il panorama nazionale e internazionale a confronto Dall'analisi svolta, senza alcuna pretesa di esaustività a livello nazionale, appare sicuramente interessante notare come, a livello geografico, vi sia una buona concentrazione di cybersecurity startup in Emilia-Romagna e in Lombardia, mentre ve ne siano poche in centro e sud Italia. Inoltre, come anticipato in premessa, poche hanno colto, anche solo a livello di marketing, l'importanza di evidenziare la compliance GDPR come punto di forza del loro prodotto. Alcune di queste realtà hanno

correttamente puntato al settore bancario e assicurativo, mentre la maggioranza di esse ha deciso di mantenere un approccio più generalista. Poche società hanno realizzato soluzioni rivolte al mondo delle applicazioni mobile o dell'IoT. Tale settore rappresenta un ambito dove nei prossimi anni sarà necessario puntare con maggiore attenzione. Grande attenzione è stata data, come era giusto che fosse, alle minacce che provengono dalla navigazione web, mentre colpisce che non siano ancora molte le società che propongano soluzioni innovative di cifratura, soprattutto se si considera l'attenzione posta dal GDPR a questo tema. Sappiamo bene però quanto sia complesso, soprattutto per una PMI, gestire a livello interno qualsiasi sistema di cifratura. Il mercato della cyber security L'espansione del mercato della cyber security è indiscutibile: il mercato globale passerà dai 105 miliardi di dollari di investimento nel 2015 ai 181 miliardi di dollari nel 2021. Se si considera che l'investimento globale nel 2004 era di 4 miliardi di dollari, questa vertiginosa crescita esponenziale del mercato deve necessariamente indurre

anche gli investitori italiani a credere seriamente in questo settore. Tuttavia, le molte operazioni fatte sul mercato nazionale hanno principalmente riguardato investimenti su società di consulenza e non di prodotto a dimostrazione che uno dei limiti principali a livello nazionale rimane quello del coraggio nel 'mettere mano al portafoglio' quando il livello di rischio aumenta. A livello internazionale, il polo di maggiore interesse oltre a quello statunitense è sicuramente quello israeliano. Il primo elemento distintivo rispetto al mercato italiano è, ovviamente, dato dal diverso approccio dei venture capitalist fin dai primi round di investimento. È evidente che un'idea può vedere la luce solo con investimenti adeguati e alcuni Paesi hanno compreso da tempo quanto sia necessario avere un approccio lungimirante accettando il rischio di perdere capitali ingenti. In secondo luogo, è sicuramente interessante notare come molte delle startup nate in un contesto diverso da quello europeo, pur non avendo alcun obbligo al riguardo, abbiano promosso soluzioni GDPR compliant: dalla gestione del data breach, a sistemi innovativi di IAM (Identity access management, dalla

cifratura e da sistemi DLP (Data Loss Prevention) fino ad arrivare a società che promuovono tool di valutazione del rischio cyber nel contesto aziendale al fine di garantire l'effettuazione di security assessment in conformità con il GDPR. I principali trend di mercato AI netto di queste considerazioni preliminari, i trend principali evidenziati da un'analisi fatta durante lo Startupbootcamp FinTech & CyberSecurity svoltosi recentemente in Amsterdam sono di triplice natura. In primoluogo, le cybersecurity startup si stanno sempre più indirizzando verso il machine learning e, più in generale all'universo AI, attraverso l'introduzione di tecniche di tipo euristico in grado di predire attacchi futuri. In secondo luogo, come naturale conseguenza del machine learning, le soluzioni più innovative di cybersecurity si stanno spostando verso il paradigma predittivo e non più verso la tradizionale modalità reattiva. L'idea non è quella della gestione dell'incident response, ma di evitare che lo stesso avvenga attraverso sistemi di prevenzione basati anche sulla creazione di sistemi innovativi ed efficaci di awareness aziendale. In terzo e ultimo luogo, partendo dal presupposto

che il cybercrime non ha confini territoriali, le cybersecurity startup stanno cercando, fin da subito, di proporsi come uno standard globale e non di limitare il loro raggio di azione al mercato nazionale di riferimento. I settori principalmente interessati sono quello aerospaziale, governativo, finanziario, telecomunicazioni e sanitario. Soprattutto su quest'ultimo settore, la necessità di proporre soluzioni efficaci in termini di sicurezza informatica si fa sempre più pressante considerato l'elevato rischio sia in termini di sicurezza che di privacy nel caso in cui una struttura sanitaria dovesse subire un cyber-attacco. Gdpr e startup Da ultimo vale la pena di evidenziare un ulteriore possibile ostacolo per la crescita delle startup evidenziato da Lenard R. Koschwitz, Senior Director di Allied For Startups (network di advocacy Europeo a favore del mondo delle Startup), il quale ha provocatoriamente affermato che il GDPR non è di aiuto alle startup. Questo, per quanto possa sembrare assurdo, vale in modo particolare per il settore della cybersecurity. I condivisibili principi della privacy by design e by default sono di difficile applicazione in un futuro sempre più orientato a

soluzioni fondate sul machine learning e sull'intelligenza artificiale. Il concetto di decisioni automatiche e di profilazione nel mondo della cybersecurity sono di basilare importanza per poter garantire l'efficienza di un sistema, ma una interpretazione troppo letterale del GDPR potrebbe interrompere sul nascere progetti potenzialmente innovativi e in linea con l'art. 32 dello stesso Regolamento Europeo. Ciò non significa che si debba promuovere la disapplicazione del GDPR per le startup, ma sicuramente si devono indicare indicazioni chiare ed efficaci come peraltro previsto dal nuovo articolo 154 bis del D.lgs. 196/2003 (novellato dal D.lgs. 101/2018) che prevede l'arrivo di specifiche linee guida per adeguarsi al GDPR per micro, piccole e medie imprese. Il mondo delle startup in Italia I3P (incubatore del Politecnico di Torino) ha osservato, in 20 anni di esperienza sul campo, che in Italia sopravvive quasi il 90% delle startup. Quasi nessuna, però, diventa grande: una su dieci ha un fatturato superiore ai 500mila euro; ma la media si avvicina a 170mila. Questo dato è in netta controtendenza non

solo con le realtà statunitensi, ma anche con quelle europee e denota due caratteristiche proprie del nostro Paese: l'estremo individualismo e l'eccesso di prudenza nella capacità di investimento. Tuttavia, il mondo delle startup deve avere coraggio se vuole innovare e deve necessariamente accettare il rischio di fallire nel suo progetto. Il fatto di minimizzare il rischio ha come conseguenza positiva la sopravvivenza della stessa realtà che progressivamente finisce per virare dal mondo dell'impresa al magmatico universo della consulenza. Viviamo, però, in un momento storico, sia dal punto di vista di evoluzione tecnologica che di compliance normativa, dove la rapidità dei cambiamenti impone un cambio di paradigma: dobbiamo realizzare prodotti e soluzioni in grado di aiutare la protezione del dato evitando di pensare che sia sufficiente una buona consulenza che avrà come risultato, nel migliore dei casi, l'indicazione della necessità di adottare quelle soluzioni tecnologiche che il nostro Paese non è in grado di produrre e che, sempre di più, sta importando dall'estero. A distanza di quasi un anno dall'entrata in vigore del GDPR e in previsione dell'emanazione

del Cybersecurity Act, è necessario comprendere come, a livello nazionale, soprattutto le PMI intendano affrontare, sulla base del principio di accountability, il nuovo paradigma di gestione del dato introdotto dal Regolamento europeo. Sotto questo profilo, è evidente che servono nuove soluzioni tecnologiche in grado di consentire un approccio rivolto, by design e by default, alla privacy, alla cyber security e più in generale alla data governance. L'auspicio è quindi che ci sia la volontà da parte dello Stato, delle grandi imprese nazionali, delle PMI e soprattutto degli startupper di intraprendere questo fondamentale e importante cambio di passo. @RIPRODUZIONE RISERVATA