GENERAZIONE C, AVVOCATI A PROVA DI FUTURO

di nicola di molfetta

STEFANO MELE

Faccia a faccia con Stefano Mele. «In Italia, la legge sul 'Perimetro di Sicurezza Nazionale Cibernetica' ha focalizzato l'attenzione sulla protezione degli asset strategici dei principali operatori pubblici e privati. Nel 2021, questa sarà un'importante sfida per i cybersecurity lawyer»

L'evoluzione tecnologica è la più grande garanzia di una «lunga ed esponenziale crescita e proliferazione della 'generazione dei *cybersecurity lawyer*'. È un processo che io – e non solo io – reputo ormai inarrestabile e irreversibile. Fermarlo è impossibile, a meno che non si voglia provare a tornare ai tempi della macchina per scrivere». **Stefano Mele** è uno di quegli avvocati che guarda avanti. Esponente di quella che potremmo definire Generazione C, nel senso di cybersecurity. Partner di Carnelutti, dove è responsabile del dipartimento di Diritto delle tecnologie, privacy e cybersecurity, nel 2014 è stato inserito dalla Nato nella lista dei suoi key opinion leader for cyberspace security. È, inoltre, il Presidente dell'Autorità per le Tecnologie dell'Informazione e della Comunicazione ("Autorità ICT") della Repubblica di San Marino e socio fondatore della

società Humint Consulting.
MAG lo ha incontrato per discutere delle opportunità e dei rischi che in un futuro sempre più digitale si presentano per gli avvocati e gli studi legali. A cominciare dalla grande questione della cybersecurity.

Avvocato Mele, la pandemia di Covid-19 ha messo in grande evidenza il tema della cybersecurity. Perché? Ci sono dati?
L'emergenza sanitaria ha posto il tema della protezione dei dati e delle informazioni in cima alla lista delle preoccupazioni di ogni operatore pubblico e privato, in quanto tutta la pubblica amministrazione e la quasi totalità delle aziende non erano pronte a una migrazione improvvisa e di massa dei dipendenti verso il telelavoro.

In che senso?
Non lo erano – e in molti casi non lo sono tuttora – sul piano tecnologico, in quanto, ad esempio, non tutti i datori di lavoro hanno provveduto ad assegnare a ogni singolo dipendente un *laptop* e uno *smartphone* per lavorare da remoto. Non lo erano – e in molti casi non lo sono tuttora – sul piano dei processi, perché la nostra cultura lavorativa, persino per i liberi professionisti, è legata ancora oggi al concetto tradizionale di "sede di lavoro". Non lo erano – e in molti casi non lo sono tuttora – sul piano della cultura della sicurezza, in considerazione degli scarsissimi investimenti che ogni operatore pubblico e privato dedica alla formazione. Infine, ancora una volta, non lo erano – e in molti casi non lo sono tuttora – sul piano della sicurezza dei dati e delle informazioni, in quanto la mancanza di tecnologie, di processi e di cultura ha fatto sì che ogni dipendente collegato dalla propria abitazione sia diventato improvvisamente (e ancor più del consueto) una vera e propria porta di accesso spalancata sui sistemi informatici e su tutto il patrimonio informativo del datore di lavoro.

La pandemia ha fatto emergere tutti quei problemi strutturali che i professionisti del settore riconoscono e segnalano da sempre...
Purtroppo però, per avere dei dati reali sulla gravità della situazione, dovremo ancora attendere. Sale giornalmente agli onori della cronaca l'enorme e costante ondata di attacchi di tipo "ransomware", che da mesi stanno flagellando tutti gli operatori pubblici e privati italiani.

Quindi le aziende e gli studi legali non erano preparati ad attivare il telelavoro e a proteggere i dati e le informazioni sensibili?
La maggior parte delle aziende e degli studi legali, come accennato in precedenza, sono ancora abituati a focalizzare la propria attenzione sul come proteggere i dati e le informazioni in una situazione di lavoro "tradizionale", ovvero prettamente statica e *on-site*. Alcuni di essi, per esigenze di business, solo negli ultimi anni hanno modificato questo approccio per permettere ad una parte dei lavoratori di svolgere la propria attività anche da remoto. La pandemia, però, ha mutato repentinamente questa dinamica, costringendo la quasi totalità degli attori pubblici e privati a far migrare gran parte della forza lavoro verso quello che impropriamente viene definito *smart working*.

> LA *CYBERSECURITY* DEVE ESSERE ANCHE UN TEMA DI *COMPLIANCE*, CHE DEVE COINVOLGERE TUTTE LE PRINCIPALI FUNZIONI AZIENDALI, PARTENDO DAL VERTICE E DAL CDA, PASSANDO PER LE FUNZIONI *LEGAL* E *SECURITY*, FINO AD ARRIVARE A OGNI SINGOLO DIPENDENTE

Il processo era in corso. Il problema è stata l'accelerazione?
Il punto di criticità è rintracciabile proprio nella repentinità di questo mutamento e – dobbiamo dirlo – in alcuni casi anche nell'impreparazione di molti di questi attori nel fronteggiare una situazione di crisi inaspettata, come è senz'altro quella pandemica legata al Covid-19. Tutto ciò pone i dati e le informazioni di questi soggetti in una situazione di enorme rischio.

Assieme alla privacy, questa materia ha integrato la *to do list* dei *compliance manager*?
Il tema della *cybersecurity* è da sempre visto come un "problema" strettamente tecnico-informatico, appannaggio, quindi, dei *security manager* e degli IT *manager*. Un problema tecnico che, pertanto, si ritiene debba essere gestito e risolto dai tecnici. Questa, però, è una visione – mi si passi il termine – da inizio del secolo scorso. Il tessuto economico di ogni nazione pulsa, oggigiorno, al ritmo e alla velocità delle connessioni ad Internet. Si alimenta dei dati e delle informazioni che vi transitano. Cresce al moltiplicarsi delle infrastrutture tecnologiche. Pensare, quindi, che la sicurezza e la protezione di tutto ciò sia solo un compito per tecnici, significa avere una percezione miope del proprio business. Per questo la *cybersecurity* deve essere, oggi più che mai, anche un tema di *compliance*, che deve coinvolgere tutte le principali funzioni aziendali, partendo anzitutto dal vertice e dal consiglio di amministrazione, passando per le funzioni *legal* e *security*, fino ad arrivare ad ogni singolo dipendente.

La tecnologia sta diventando strumento fondamentale per l'esercizio della professione, ma sarà sempre più anche oggetto della professione legale. Perché?
Se ci fermiamo a riflettere, quasi tutto ormai è o può essere digitalizzato. Nel mondo odierno – e ancor più nel prossimo futuro – la tecnologia svolgerà un ruolo sempre più centrale in ogni aspetto della nostra vita sociale e lavorativa, nei processi produttivi, nella fornitura di beni e servizi, così come in tanto altro ancora. Il mondo della professione legale, ovviamente, non fa eccezione.

Con quali peculiarità?
Se è vero che da sempre gli avvocati supportano con i loro servizi ogni settore regolamentato dalle norme, focalizzandosi ciascuno nel proprio campo di vocazione, quello delle tecnologie e della *cybersecurity* è il primo nella storia ad essere completamente trasversale a ogni altro. Infatti, se tutto è digitalizzato e le tecnologie svolgono quel ruolo cardinale che gli riconosciamo, la loro comprensione e sicurezza è ovviamente prioritaria in ogni settore, al di là del campo di applicazione.

Il che cambia l'approccio che da verticale diventa orizzontale?
Ho sempre pensato che, per svolgere al meglio la professione nel campo del diritto delle tecnologie e della *cybersecurity*, occorra padroneggiare qualsiasi settore del diritto in cui le tecnologie abbiano un ruolo. Non può bastare, quindi, essere esperti di contrattualistica in ambito tecnologico o di privacy, se si svolge la professione nel campo del diritto civile, oppure di crimini informatici, se ci si muove nel settore del diritto penale. Si deve guardare alla materia con un approccio omnicomprensivo, ovvero, appunto, in maniera orizzontale.

Carnelutti come si sta muovendo?
Carnelutti Law Firm, grazie alla sensibilità

> LA TECNOLOGIA CON IL PASSARE DEL TEMPO INVADERÀ E MODIFICHERÀ TUTTI I SETTORI DEL DIRITTO, DIVENTANDO SEMPRE DI PIÙ L'OGGETTO PRINCIPALE DELLA NOSTRA PROFESSIONE

del managing partner **Luca Arnaboldi**, sin dal 2010, ha condiviso con me questa visione della professione legale – al tempo davvero "rivoluzionaria" – e ha puntato moltissimo sulla creazione di uno specifico dipartimento focalizzato, in maniera orizzontale, proprio sul diritto delle tecnologie, sulla privacy e sulla *cybersecurity*, vedendo, peraltro, nella multidisciplinarietà un punto di forza per rendere ai nostri clienti un servizio davvero completo e a valore aggiunto.

Quali sono le principali normative nel settore della *cybersecurity* che impattano le aziende italiane?
Sul piano normativo, il settore della *cybersecurity* ha radici lontane, che sono intimamente legate al tema della protezione dei dati personali e del *know-how* pregiato delle aziende. Il vero cambio di passo lo si è avuto solo nel 2017, quando l'Unione europea, all'interno della sua *cybersecurity strategy*, si è posta degli obiettivi strategici anche in campo normativo tanto ambiziosi, quanto coerenti con le attuali esigenze. Il cosiddetto GDPR, la Direttiva NIS e il *Cybersecurity Act* sono solo una parte degli impianti normativi – forse i più famosi – che il legislatore europeo ha posto in essere per innalzare i livelli di sicurezza cibernetica e proteggere la digitalizzazione dei Paesi Membri. Va detto che in Italia, di recente, la legge sul 'Perimetro di Sicurezza Nazionale Cibernetica' ha focalizzato l'attenzione sulla protezione degli *asset* strategici dei principali operatori pubblici e privati. Nel 2021, pertanto, questa sarà un'importante sfida per tutti gli attori convolti e i *cybersecurity lawyer* saranno tra i principali protagonisti.

La digitalizzazione delle aziende implica un cambio di pelle anche da parte dei loro consulenti legali?
Il mondo degli avvocati e dei consulenti legali deve ancora evolvere e adeguarsi a pieno a questo scenario. Se è ormai acclarato che un eccellente avvocato debba anzitutto saper "parlare la lingua del cliente", in questo settore ciò significa riuscire a parlare non solo quella del business e dei legali, ma anche quella della *security*, dell'IT *security*, dell'*audit*, del *procurement*, dell'HR e così via. La *cybersecurity*, infatti, è la massima espressione della interdisciplinarità e della multidisciplinarietà, perché rappresenta il tema di base per qualsiasi processo all'interno delle aziende, così come delle pubbliche amministrazioni. Soltanto così il nostro lavoro nel settore della *cybersecurity* può davvero creare valore e non essere considerato un freno.

Quali sono le frontiere per cui ci si deve preparare?
L'intelligenza artificiale, l'automazione e la robotica saranno senz'altro i principali *game changer* che caratterizzeranno la frontiera a noi più prossima e che, grazie anche alla cosiddetta *Internet of Things* e alle reti iperveloci di nuova generazione (es., 5G e 6G), stravolgeranno il mondo del business e del lavoro. Molti si concentrano sul ben noto assioma che, a causa della prossima rivoluzione tecnologica alcuni posti di lavoro andranno persi e molti altri verranno creati. Pochi riflettono, invece, sull'unica certezza reale, ovvero che quasi tutti i modi di lavorare cambieranno. Pertanto, a mio avviso, dobbiamo ragionare fin da subito, affinché quella del prossimo futuro sia una storia di miglioramento delle attività lavorative grazie alle nuove tecnologie e non di sostituzione. Questa è la vera frontiera a cui ci si deve preparare, che vedrà la 'generazione dei *cybersecurity lawyer*' impegnata in prima linea.