filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Avvocati: innovazione tecnologica e cybersecurity, un equilibrio in continua evoluzione

26 Maggio 2021
Deborah Caputo, Cesare del Moro

Abstract
A causa della situazione pandemica che stiamo affrontando, la professione legale è protagonista di un inevitabile cambiamento sostanziale e strutturale; in tale processo di evoluzione ha assunto un ruolo fondamentale la tecnologia come indispensabile strumento di prosecuzione dell'attività e, al contempo, imprescindibile fattore di visione e rinnovamento della stessa. L'incidenza della tecnologia sulla gestione pratica della professione e della relativa struttura organizzativa, che sta migrando verso la dematerializzazione, richiede però un alto livello di attenzione verso la protezione dei dati e delle informazioni custodite dallo studio legale e conseguentemente l'adozione di misure di sicurezza – tecniche e organizzative – idonee a ridurre i rischi di violazione e mitigare le conseguenze negative derivanti. Per massimizzare gli effetti positivi della digitalizzazione della professione non si può prescindere dalla consapevolezza delle criticità e vulnerabilità del sistema adottato e dalle nozioni cardine dell'efficienza informatica e della protezione dei dati. Riflettendo su rischi e opportunità della digitalizzazione, l'articolo si propone di offrire qualche spunto pratico per affrontare in sicurezza la professione in modalità "digitale".
Due to pandemic situation we are facing, the legal profession is protagonist of an inevitable substantial and structural change; in this evolution process, technology has taken on a fundamental role as an indispensable tool for the business continuity and, at the same time, an essential factor for its vision and renewal. The impact of technology on the practical management of the profession and its organizational structure, which is migrating towards dematerialization, requires, however, a high level of attention to the data and information protection held by the law firm and consequently the adoption of security measures - technical and organizational - suitable to reduce the risks of breach and mitigate the negative consequences arising. To maximize the positive effects of the digitalization of the profession, one cannot be ignored the awareness of the criticality and vulnerability of the system adopted and the main principles of information efficiency and data protection. Reflecting on digitalization risks and opportunities, the article aims to offer some practical ideas to safely address the profession in "digital" way.

Indice:

1. Sicurezza del patrimonio informativo dello studio legale: tra esigenza ed obbligo

Ogni studio legale, piccolo o grande che sia, detiene e gestisce un ingente volume di informazioni, spesso di natura sensibile, come dati particolari o giudiziari dei clienti, o comunque particolarmente delicate, comprese quelle societarie riservate (come, ad esempio, eventuali prototipi, contratti relativi a una certa operazione o i criteri di pianificazione strategica di business condivisi dalle società clienti, *etc.*).

Pertanto, garantire la sicurezza del patrimonio informativo conservato dallo studio legale costituisce per l'avvocato un'esigenza prioritaria, in linea con i doveri di segretezza e riservatezza che il professionista è deontologicamente tenuto a rispettare. Quando poi le informazioni detenute rendono una persona fisica identificata o identificabile tale esigenza trova la propria fonte diretta nella normativa in materia di protezione dei dati personali, con il conseguente obbligo per lo studio legale – al pari di ogni altra organizzazione che tratta dati personali – di uniformarsi ai principi e requisiti dalla stessa definiti.

2. Luci e ombre della digitalizzazione

La necessità per l'avvocato di attivarsi per assicurare un'adeguata protezione del patrimonio informativo a sua disposizione ha assunto una maggiore o, meglio, diversa rilevanza nel contesto dell'emergenza sanitaria che stiamo ancora affrontando, nell'ambito della **quale la digitalizzazione della professione si è fatta intensa e veloce, forse più di quanto gli avvocati fossero preparati ad affrontare, sulla spinta della inevitabile dematerializzazione e delocalizzazione dello studio**.

Intendiamo per digitalizzazione la migrazione delle attività del professionista verso un contesto completamente digitale/virtuale e l'adozione di processi remotizzati e per dematerializzazione l'abbandono dello studio come struttura fisica basata su sistemi cartacei e server in sede, nonché dell'interazione fisica come impostazione predefinita, con la conseguente delocalizzazione delle attività professionali e dei trattamenti di dati personali e informazioni (cfr. G. Ziccardi, *Delocalizzazione e dematerializzazione dello studio legale*, Giuffrè, 2020; report dell'Osservatorio Professionisti e Innovazione Digitale del Politecnico di Milano sul ruolo delle tecnologie digitali nel processo di cambiamento che sta investendo il mondo delle professioni, maggio 2020).

Tali fenomeni, che coinvolgono l'intera organizzazione della professione – dalle modalità di svolgimento delle attività, alla tipologia degli strumenti utilizzati, ai rapporti con clienti e colleghi, per arrivare alla tenuta delle udienze da remoto – hanno determinato necessariamente una **nuova visione della professione legale, imprescindibilmente legata alla tecnologia, facendo sorgere, al contempo, il bisogno di raggiungere un livello di sicurezza più elevato** (anche nell'esecuzione delle operazioni quotidiane più semplici e ordinarie).

Infatti: il ricorso alle soluzioni tecnologiche se, da un lato, ha consentito ai professionisti di proseguire "senza interruzioni" e in modo efficiente la propria attività, dall'altro lato, **ha esposto il relativo patrimonio informativo ai rischi connaturati ad una digitalizzazione improvvisa e imprevista e a uno stato dell'arte debole e vulnerabile** in ragione delle ridotte risorse (finanziarie e di tempo) fino a oggi investite, nella maggior parte dei casi e soprattutto nelle realtà più piccole, per garantire misure efficaci di sicurezza e protezione di tale patrimonio informativo e di prevenzione di eventuali incidenti/eventi pregiudizievoli della riservatezza, integrità e disponibilità dei dati. Circostanza, questa, che ha ampliato la superficie di attacco a disposizione dei cybercriminali, rendendo gli studi legali un bersaglio più esposto.

Una violazione della sicurezza dei dati personali e delle informazioni può avere degli effetti legali, economici e reputazionali devastanti per gli stessi studi e, naturalmente, per i clienti. Per questo è fondamentale che gli studi si dotino di una serie di misure e policy finalizzate a scongiurare il rischio di eventuali attacchi – accidentali o intenzionali – al patrimonio informativo e le plurime conseguenze negative correlate.

3. Digitalizzazione e sicurezza a tappe

Per quanto necessario e inevitabile lo sviluppo del processo di digitalizzazione non può prescindere, nel concreto, dalle risorse ed esigenze di ogni studio o singolo professionista. **Tuttavia, anche se la dimensione dello studio è un elemento che può fare la differenza, l'adozione di un primo "pacchetto base" di regole/azioni può assicurare a tutti un rapido e significativo beneficio per la qualità dell'assetto di sicurezza dello studio, che sarà possibile incrementare procedendo a livelli**.

L'indispensabile	**Il (caldamente) consigliato**
Antivirus *per proteggere i dati da malware*	Suite di sicurezza professionali *dotate di moduli dedicati alla protezione per specifiche minacce (es. ransomware)*
Email - PEC *dotate di misure di sicurezza e capienza adeguate*	Gestore Password *per memorizzare le password in un luogo sicuro e, al contempo, facilmente accessibile*
Firma(e) digitali, *anche remote, utilizzabili anche in caso di incidente fisico a dispositivi collegati*	VPN *per garantire la riservatezza delle comunicazioni anche su reti non verificate*
Connettività (telefono internet e centralino) *sottoposte ad un monitoraggio che rilevi tempestivamente le intrusioni*	Crittografia *per garantire la sicurezza dei dati, in transito e a riposo, correttamente configurata*
Messaggistica *adeguata, tra le altre cose, al livello di riservatezza dei messaggi veicolati*	Videoconferenze *dotate di misure di sicurezza e comprovata affidabilità contro intrusioni e illecita conservazione di dati*
Backup e Disaster Recovery *efficientemente ripristinabili e periodicamente testati per garantire la continuità operativa*	Cloud *dotato di misure di sicurezza e spazio adeguati, correttamente configurato, anche per evitare la propagazione di malware*
Scanner e Multifunzione *dotati di misure di sicurezza adeguate a proteggere le informazioni gestite ed eventualmente immagazzinate nella memoria del dispositivo*	Tracciabilità e condivisione *idonee alla ricostruzione di responsabilità con log management*

Alziamo l’asticella

Separazione dei Dati (SOD) e delle Reti *per ridurre l’impatto di violazioni o incidenti sempre possibili.*	Scalabilità e Adattabilità degli strumenti. *L’ottimizzazione dei supporti e dei processi permette di rispettare più agevolmente i principi di privacy by design e by default*
Monitoraggio su dati personali e avvisi di possibile compromissione *per gestire in modo più efficace eventuali necessarie contromisure a possibili breach*	Polizza cyber security *per trasferire, nei limiti della polizza, il rischio di danni derivanti da data breach*
Gestionali pratiche e fatturazione *dotati di misure di sicurezza e caratteristiche di interoperabilità per ridurre eventuali rischi sui dati trattati*	DPO *in quanto soggetto indipendente, autonomo e competente, che sorveglia i processi di sviluppo e adeguamento per una migliore protezione dei dati e conseguente tutela dello studio*
Controllo centralizzato dei dispositivi (MDM) *per rendere più efficiente la gestione degli asset e potere applicare misure di sicurezza tecniche a livello centralizzato*	Personale IT consapevole delle esigenze dello studio/del professionista per *sviluppare soluzioni efficaci e sicure e ridurre i rischi di una errata configurazione dei sistemi*
Gestione di eventuali ‘‘consensi’’ tramite sistemi digitali (newsletter, cookie, *etc.*) *per ottimizzare il trattamento dei dati e poter gestire l’esercizio dei dati degli interessati con maggior sicurezza*	Controllo filiera consulenti e fornitori *e formalizzazione dei relativi ruoli e responsabilità tramite appositi atti giuridici anche per contenere il rischio che eventuali “breach” dell’organizzazione dei consulenti e fornitori si riflettano sulla dimensione fisica e tecnologica dello studio*

4. Non c’è sicurezza senza consapevolezza

L’adozione delle misure appena ricordate non può tuttavia prescindere dal fattore umano.

Le persone costituiscono spesso l’anello debole dei processi di sicurezza soprattutto quando non vengono dati loro i giusti strumenti per capire quali effetti potrebbe avere il loro comportamento sui sistemi. In media, un utente non qualificato sottovaluta o ignora le precauzioni di sicurezza che gli vengono suggerite/impartite.

La maggior parte degli attacchi su rete, così come gli incidenti di sicurezza e i numerosi casi di violazione dei dati, sono causati da – diverse – condotte umane non adeguate: si pensi, ad esempio,
all'invio per errore di una e-mail contenente informazioni estremamente riservate di un cliente;
all'utilizzo non corretto del meccanismo delle password (condivisione di password tra più utenti, utilizzo di password senza scadenza o facilmente individuabili o per più servizi on-line);
alla poca sensibilità sulla criticità della dimensione digitale del dato (con la conseguente condivisione e conservazione di documenti contenenti dati particolari o informazioni sensibili tramite canali non protetti);
all'utilizzo di reti pubbliche, al mancato aggiornamento dei dispositivi, *etc.*

Tali condotte derivano dalla mancata conoscenza di nozioni di sicurezza informatica e della normativa in materia di protezione dei dati personali; conoscenza che, oggi, l'avvocato non può escludere dalla propria formazione anche per evidenti ragioni deontologiche di segretezza, riservatezza e aggiornamento professionale (considerata anche la commistione di aspetti tecnici e giuridici che alcune materie, come la privacy, necessariamente comportano).

Acquisire una sensibilità verso tali tematiche (e, nel caso di realtà più strutturate, diffonderla tra i dipendenti e collaboratori) risulta essenziale per tutelare il proprio sistema informativo : solo la consapevolezza delle lacune esistenti, delle misure adottate e da adottare e del peso delle proprie condotte può contenere il rischio di eventi pregiudizievoli e consentire alla categoria di affrontare l'evoluzione in corso in modo ottimale, individuando eventuali criticità e massimizzando le utilità connesse all'impiego della tecnologia, quali ad esempio riduzione dei tempi, maggiore flessibilità, facilitazione e snellimento del flusso di lavoro e della comunicazione, ed evitare ad ogni professionista di esporsi a eventuali responsabilità.

TAG: *avvocato, cybersecurity, digital transformation*
