CULTURA E DIRITTI
PER UNA FORMAZIONE GIURIDICA

SCUOLA SUPERIORE DELL'AVVOCATURA
FONDAZIONE DEL CONSIGLIO NAZIONALE FORENSE

rivista trimestrale • anno III • numero 4 • ottobre-dicembre 2014

PISA
UNIVERSITY
PRESS

Indice

Approfondimenti

Cultura e professione

L'avvocatura dei giovani

DOI 10.12871/97888674151683

Something's got to give: breve comparazione tra l'approccio americano ed europeo al *cloud computing*, soluzioni pratiche*

Nathan M. Crystal e Francesca Giannoni-Crystal

Può uno studio legale internazionale, con uffici negli USA e in Europa, adottare un'unica policy per l'utilizzo del *cloud computing*? La risposta è affermativa, ma con alcuni distinguo e dei consigli pratici sotto forma di check list.

Un'organizzazione internazionale che utilizza il *cloud computing* (o nuvola informatica) deve confrontarsi con problematiche diverse a seconda di dove viene utilizzata questa tecnologia (per esempio se negli Stati Uniti o in Europa), in quanto il concetto e la regolamentazione inerente alla protezione dei dati personali (o privacy) divergono, e non di poco, da Paese a Paese. Il nostro recente articolo "*Something's got to give" - Cloud Computing as Applied to Lawyers - Comparative Approach US and EU and Practical Proposals to Overcome Differences*[1], individua le differenze più importanti tra l'approccio americano ed europeo alla privacy in relazione al *cloud computing* e identifica le diverse problematiche etiche che gli avvocati dei sue sistemi debbono tenere in considerazione nell'adozione del *cloud*.

I due diversi approcci alla privacy, che trovano forse la loro origine in ragioni di ordine filosofico o storico, hanno fatto sì che in Europa (dove la privacy è un diritto fondamentale) si addivenisse a una legge generale per la protezione dei dati personali – la quale regola raccolta, trattamento, trasferimento e eliminazione dei dati personali; attualmente incentrata sulla Direttiva 95/46/EC, ma presto sostituita dal nuovo Regolamento Europeo sulla protezione dei dati personali – mentre negli USA si approvassero unicamente leggi privacy settoriali[2]

* Quest'articolo è un adattamento in lingua italiana di un articolo in inglese che gli autori hanno recentemente pubblicato: N.M. Crystal - F. Giannoni-Crystal, *Reconciling US and EU Approaches to Cloud Contracts*, in *22 PL&B International*, October 2014, Issue 131, www.privacylaws.com. Si ringrazia l'Avv. Federica Romanelli (Foreign Legal Consultant in New York) per il preziosissimo aiuto in fase di trasposizione in italiano di quest'articolo, originariamente in inglese.

1 N.M. Crystal - F. Giannoni-Crystal, "*Something's got to give" - Cloud Computing as Applied to Lawyers - Comparative Approach US and EU and Practical Proposals to Overcome Differences*, om *Opinio Juris in Comparatione*, I-1/2014, disponibile a http://www.opiniojurisincomparatione.org/

2 Vedi *Health Information Portability and Accountability Act* (HIPAA) e *Fair and Accurate Credit Transactions Act* (FACTA). HIPAA si applica nel settore medico/ospedaliero e defi-

ovvero limitate alla *data breach* (cioè leggi che regolano i casi in cui vi è stata una violazione della sicurezza dei dati).

Per consentire il trasferimento di dati dall'Europa agli Stati Uniti, nel 2000 la Commissione Europea ha espresso un'opinione di "adeguatezza" *ex* art. 25 (6) della Direttiva 95/46/EC per le organizzazioni americane partecipanti allo schema "*Safe Harbor*"; tutti gli Stati membri dell'Unione Europea sono vincolati da questa dichiarazione di "adeguatezza"[3]. L'accordo di "*Safe Harbor*" è applicabile anche ai gestori americani di *cloud* ("*cloud provider*" o "*provider*")[4]. Il Gruppo di lavoro Articolo 29 ha avuto modo di chiarire che la Direttiva per la Protezione dei Dati Personali «è applicabile in tutti i casi in cui i dati personali sono trattati in conseguenza dell'utilizzo di un servizio di *cloud computing*».

La legge privacy americana non comporta grandi criticità nella scelta di adottare il *cloud*: salvo certi settori (come, per esempio, quello del trattamento dei dati sanitari)[5], la normativa statunitense impone esclusivamente il rispetto delle disposizioni previste per i casi di violazione di dati personali (c.d. "*security breach law*"). Al contrario, la privacy europea richiede un'analisi e un impegno significativi quando si adotta il *cloud.* Due sono le definizioni della Direttiva che rilevano per il *cloud computing*: quella di "responsabile del trattamento" (articolo 2(d)) e quella di "incaricato del trattamento" (articolo 2(e)). Uno studio legale (così come altra organizzazione) che utilizzi il *cloud* è senza dubbio "responsabile del trattamento" ed è, pertanto, chiamato a rispondere per qualsiasi violazione della normativa da parte dell'incaricato al trattamento. Il ruolo del *cloud provider* non è, invece, definibile con altrettanta certezza.

---

nisce chi può avere accesso alle informazioni mediche (di solito unicamente il personale sanitario e chi lo coordina). FACTA, che si applica al settore bancario e finanziario, protegge le informazioni finanziarie e creditizie dei consumatori dai rischi di violazione informatica.

[3] Il 18 giugno 2014, la Irish High Court ha rinviato in via pregiudiziale alla Corte di Giustizia Europea una serie di questioni riguardanti l'applicazione dei principi del Safe Harbor. Il nodo centrale è se i giudici nazionali siano "assolutamente vincolati" dalla dichiarazione di una società di partecipare al Safe Harbor, o se questi possano comunque verificare se, nel caso concreto, i dati personali siano effettivamente protetti conformemente allo standard europeo. *Schrems vs. Data Protection Commissioner* (C-2013 765). Vedi: http://www.technethics.com/are-european-judges-still-absolutely-bound-by-the-safe-harbor/

[4] Il Gruppo di Lavoro Articolo 29 (Opinione 05/2012) ed il US *Department of Commerce's International Trade Administration* (ITA) (*Clarifications Regarding the US-EU Safe Harbor Framework and Cloud Computing*) hanno espresso opinioni contrastanti riguardo all'applicabilità del Safe Harbor al *cloud computing*. Per il primo (che, ricordiamo, è un organismo consultivo e indipendente istituito dall'art. 29 della Direttiva 95/46/EC) «la sola autocertificazione di adesione all'accordo Safe Harbor potrebbe non essere sufficiente se la nuvola informatica non pone in essere un efficace sistema di protezione dei dati personali», mentre per il secondo «l'adesione al Safe Harbor continua a certificare che gli enti americani approvati, indipendentemente dal fatto che operino nell'industria del *cloud*, rispettano il principio di adeguatezza stabilito dalla Direttiva».

[5] *Health Insurance Portability and Accountability Act*, HIPAA, vedi nota n. 3.

In una nuvola privata, il *provider* è esclusivamente un "incaricato del trattamento", mentre in una nuvola pubblica – dove il *cloud provider* ha un controllo maggiore sui dati processati, nonché una maggiore autonomia nella definizione dello scopo e dei mezzi utilizzati per il trattamento – il *provider* potrà essere considerato anche responsabile del trattamento. Per tale motivo, i gestori delle infrastrutture dei servizi o di *social network* debbono considerarsi quali "responsabili del trattamento" ai fini della normativa europea. Tali conclusioni trovano conforto in due opinioni pubblicate dal Gruppo di Lavoro Articolo 29. Nell'Opinione 1/2010, il Gruppo di Lavoro esprime il proprio parere riguardo alla relazione tra responsabile e incaricato del trattamento. Nell'Opinione 5/2012, che tratta del *cloud computing*, il Gruppo di Lavoro applica tali concetti alla nuvola informatica: «Il cliente *cloud* determina la finalità ultima del trattamento e decide in merito all'esternalizzazione di tale trattamento e alla delega ad un'organizzazione esterna delle attività di trattamento, in tutto o in parte. Il cliente *cloud* agisce pertanto in qualità di responsabile del trattamento dei dati». Il Gruppo di Lavoro ritiene che, in linea generale, i *cloud provider* sono incaricati del trattamento: «Quando fornisce gli strumenti e la piattaforma, agendo per conto del cliente *cloud*, il fornitore *cloud* è considerato alla stregua di un incaricato del trattamento».

L'interazione tra l'utilizzatore del *cloud* e il *cloud provider* (o meglio i diversi *cloud provider*, visto che è sempre più comune che un servizio sia gestito da più fornitori) fa sorgere problematiche molto complesse riguardo alle responsabilità dei vari attori e all'individuazione della legge applicabile. In alcuni casi, il *cloud provider* è un co-responsabile o il responsabile di un diverso trattamento, il che rende necessario – parliamo qui specificamente di studi legali – che il cliente dell'avvocato dia un consenso ulteriore rispetto a quello prestato per il trattamento da parte dello studio legale. Si consideri un altro problema: se uno studio legale (parliamo ovviamente di uno studio legale extra EU) non fosse già soggetto alla normativa privacy europea, esso potrebbe esservi assoggettato in virtù dell'uso di un *cloud* che utilizza "strumenti" situati in Europa. L'articolo 4 della Direttiva impone, infatti, l'applicazione della normativa europea quando: (a) il trattamento è «effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; …[O] (c) il cui responsabile […] ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro»[6].

[6] Il 13 maggio 2014, la Corte di Giustizia Europea ha statuito che la normativa europea per la protezione dei dati personali deve applicarsi anche a quei motori di ricerca che hanno una filiale o una società collegata nell'UE che ivi venda spazi pubblicitari, indipendentemente da dove siano localizzati i loro *server*. Causa C131/12 (meglio nota come "diritto all'oblio"). La proposta di Regolamento Europeo sulla protezione dei dati personali amplia l'ambito di applicazione territoriale; ciò avrà un notevolissimo impatto sulle società americane (tra cui anche studi legali e *cloud providers*). Il Regolamento si applicherà, infatti, al trattamento dei

Tuttavia, quando si applicano tali disposizioni al *cloud computing*, una domanda sorge spontanea: "Dove è localizzata la nuvola?". L'Opinione 8/2010 del Gruppo di Lavoro Articolo 29 suggerisce che la localizzazione dei dati non è fondamentale perché «è sufficiente che il responsabile del trattamento effettui il trattamento nel contesto di uno stabilimento nell'UE o che i mezzi rilevanti siano situati sul territorio dell'UE per fare scattare l'applicazione del diritto dell'UE» Mentre questa specificazione è utile per quei responsabili del trattamento "stabiliti" in un paese europeo, essa non chiarisce la situazione in quei casi (es., studio legale americano senza sedi europee) in cui i responsabili del trattamento non sono stabiliti nell'UE (né utilizzano strumenti in Europa) ma usano un *cloud* che – esso sì – utilizza strutture (ad esempio, *server*) in Europa. Come se non bastasse, per complicare la questione, non è sempre possibile per gli utenti della nuvola sapere dove sono localizzati tutti i *server* e dove, in particolare, siano custoditi i loro dati.

Tutti questi aspetti – discussi estensivamente nel nostro articolo sopra citato – dovrebbero essere verificati come descritto nel prosieguo.

Gli aspetti da considerare quando si adotta il *cloud*

Lo schema che segue è stato elaborato per la specifica situazione degli studi legali internazionali tuttavia può utilizzarsi, *mutatis mutandis*, anche da parte di altre organizzazioni.

1. Identificazione della tipologia/e di servizi cloud che lo studio intende utilizzare e analisi dei costi/benefici

Preliminarmente diciamo che esistono tre modelli di servizio *cloud*: "Software as a Service" (SaaS, cioè specifici *software* erogati come servizi di *cloud*), "Platform as a Service" (PaaS, cioè piattaforme fornite via internet come servizio), "Infrastructure as a Service" (IaaS, cioè infrastrutture *cloud* rese disponibili come servizio). Queste tipologie si possono sviluppare tramite quattro tipologie: *cloud* privata, pubblica, ibrida, di gruppo. Di seguito ci concentreremo sul SaaS (che generalmente è offerto su nuvole pubbliche), in quanto questa modello risulta il tipo di servizio più utilizzato dagli studi legali. Le indicazioni di cui sotto sono, comunque, generalmente applicabili a tutti i modelli di servizio e a tutte tipologie di *cloud*.

Per ciascun servizio SaaS che uno studio legale intende utilizzare, è opportuno effettuare un'analisi costi/benefici per determinare se l'adozione del servizio abbia senso dal punto di vista economico. Riteniamo che sia importante

dati personali effettuato da: (i) persone fisiche o giuridiche responsabili oppure incaricati del trattamento dei dati personali nell'UE, *e* (ii) a quei responsabili *non* stabiliti nell'UE, quando il trattamento riguarda: (a) l'offerta di servizi a residenti dell'UE; o (b) il controllo del loro comportamento. Articolo 3.

effettuare tale valutazione prima della stima dei rischi etici e legali. Se l'utilizzo del servizio non è conveniente, è inutile passare alla valutazione dei rischi e all'analisi per minimizzarli. Alcuni aspetti della valutazione del beneficio economico sono quantificabili, mentre altri lo sono meno (pensiamo all'aspetto della comunicazione più veloce con il cliente o alla comodità d'uso di banche dati accessibili ovunque). La posta elettronica è probabilmente il servizio *cloud* maggiormente utilizzato dagli studi legali: infatti, mentre si può discutere la convenienza di altri servizi, quella della posta elettronica è fuori discussione. Il costo dell'e-mail è minimo, o addirittura inesistente, mentre i benefici in termini di efficienza, speditezza, risparmio di costi per via dell'eliminazione di francobolli, carta e personale, sono notevoli. Un ulteriore beneficio dell'adozione del *cloud* consiste nel fatto che questi consente di essere sempre al passo con l'avanzare della tecnologia. Tenersi al passo con la tecnologia, per gli avvocati americani, è parte dal dovere di competenza professionale ed è ora espressamente previsto dal Commento [8] dell'articolo 1.1 delle Regole Deontologiche tipo[7] emanate dall'American Bar Association (ABA). Inoltre, di solito, il *cloud* consente l'uso delle tecnologie più all'avanguardia e degli ultimi aggiornamenti, che sono automatici, così come automatici sono i *backups*.

2. Identificazione dei rischi associati con lo specifico servizio

Gli avvocati americani sono soggetti a molteplici doveri deontologici quando si tratta di utilizzare servizi di *cloud* e sono tenuti ad identificare quei rischi che potrebbero tradursi in violazioni etiche, responsabilità legali, o danni alla reputazione dello studio. Nello specifico, i principali doveri deontologici da considerare nell'adozione e uso del *cloud* sono i seguenti:

– Competenza.
– Comunicazione con il cliente, che include il dovere di informare il cliente in caso di compromissione del sistema informatico.
– Riservatezza riguardo ai dati del cliente, che impongono all'avvocato di fare quanto ragionevolmente necessario per evitare la divulgazione non autorizzata delle informazioni riguardanti i propri clienti.
– Mantenimento, conservazione e restituzione, al termine dell'incarico, delle cose di proprietà del cliente.
– Supervisione del lavoro di avvocati e personale non legale, ivi inclusi i c*loud provider*.

Gli avvocati europei sono soggetti a doveri professionali di tipo simile.

La violazione di questi doveri professionali si può tradurre in responsabilità professionale o in violazione deontologica o in entrambe. Inoltre, un trattamento improprio dei dati dei clienti può danneggiare la reputazione dello studio,

[7] http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html.

con conseguente perdita di clientela. Oltre al rischio di violazione dei doveri deontologici sopraelencati, l'uso del *cloud* comporta ulteriori pericoli: vi sono "rischi legali" (come, per esempio, inadempienza contrattuale verso il cliente), rischi di violazione di norme sulla sicurezza dei dati (come, per esempio, violazione di una *security breach law* e violazioni privacy) e rischi di natura "tecnica", sia interni che esterni allo studio.

L'utilizzo di un servizio SaaS comporta i seguenti rischi "esterni":

– divulgazione non autorizzata d'informazioni a seguito di violazione del sistema di sicurezza del *cloud provider*;
– diffusione di dati risultante da erronea gestione, da parte del *provider*, di richieste "ufficiali" di fornire informazioni (per esempio, *subpoena* nel sistema statunitense)[8];
– mancanza di chiarezza circa la proprietà dei dati e licenza d'uso dei dati al *cloud provider*;
– temporanea indisponibilità dei dati dovuta a mancanza di collegamento *internet*, a manutenzione o interruzione del sistema;
– perdita definitiva dei dati a seguito di fallimento del *provider*;
– rischi derivanti dalla localizzazione geografica dei *servers*, dovuti al fatto che i dati si trovano in paesi con differente regolamentazione privacy;
– problemi inerenti la restituzione dei dati a seguito della cancellazione del contratto.

Anche se è possibile identificare i rischi in linea generale, si consideri che situazioni particolari potrebbero comportare ulteriori rischi specifici[9].

Per quanto concerne i "rischi interni", questi possono scaturire dalla mancata adozione da parte dello studio legale di procedure e criteri utili a eliminare o ridurre i rischi esterni di cui sopra. Si noti che gli studi legali debbono gestire le criticità interne inerenti il trattamento dei dati personali dei clienti indipendentemente dall'utilizzo di *cloud*. Si debbono, infatti, identificare mezzi idonei alla eliminazione o minimizzazione dei rischi derivanti dal trattamento interno di dati; per esempio stabilendo quali dispositivi elettronici gli avvocati dello studio possono utilizzare per comunicare con i clienti e quali siano le procedure da seguire per la distruzione di quegli apparecchi.

[8] Il *subpoena* è un ordine – emesso da una corte, un'agenzia governativa o da avvocati (quali ufficiali della corte) – in connessione con un procedimento che impone la comparizione di un testimone o la produzione di documenti o altro. Come si comprende dal nome, l'ordine è assistito da sanzione in caso di inottemperanza.

[9] Per esempio, sono richieste particolari precauzioni per il caso in cui la pubblica amministrazione (o un appaltatore operante per la stessa) tratti dati inerenti sulla sicurezza nazionale. Allo stesso modo, HIPAA (vedi *supra* nota n. 3) prevede l'adozione di particolari precauzioni.

3. Eliminazione o minimizzazione dei rischi

Gli studi legali dovrebbero porsi delle domande specifiche e informarsi con diligenza per valutare i rischi connessi all'utilizzo di *cloud computing*. Ecco una check list di questi interrogativi:

- Qual è la reputazione del *provider* per qualità e sicurezza? È stato consigliato da ordini professionali o è comunque stato raccomandato o certificato da enti o organizzazioni di categoria?
- Quali sono le misure adottate dal *provider* per proteggere i dati da accessi non autorizzati?
- Quali sono gli *standard* di sicurezza di quella *industry*?
- Il *provider* in questione è conforme a quegli *standard*?
- Cosa prevede il contratto di *cloud* rispetto alle azioni che il *provider* è tenuto a porre in essere per mitigare le conseguenze di una violazione dei dati?
- Cosa prevede il contratto di *cloud* sulla notifica di una violazione dei dati?
- Lo studio legale adotta procedure interne che obbligano ciascun avvocato dello studio e ciascun dipendente dello stesso a informare i responsabili in caso di violazione dei dati?
- Cosa prevede il contratto di *cloud* per il caso in cui al *provider* sia notificata una richiesta di informazioni, per esempio un *subpoena* o un *warrant*?[10]
- Cosa dispone il contratto di *cloud* con riferimento alla proprietà dei dati, all'utilizzo degli stessi da parte del *provider* e alla licenza a terzi da parte del *provider*? Attenzione: il contratto deve prevedere che lo studio legale o il cliente di quest'ultimo, a seconda dei casi, è il proprietario dei dati. Il contratto deve anche stabilire che il *provider* può subappaltare a terzi parte del servizio solo con il consenso espresso dello studio legale o del cliente, a seconda di chi è il proprietario dei dati. Nel caso in cui il contratto di *cloud* contenga una clausola non negoziabile che consente al *provider* di operare in *outsourcing*, lo studio legale è tenuto – per i propri doveri deontologici – a ottenere il previo consenso del cliente a tal fine. Ciò sembra necessario anche per ottemperare alla normativa europea di protezione dei dati personali. Nel diverso caso in cui contratto di *cloud* autorizzi il *provider* ad utilizzare i dati, si dovrà valutare, ordinamento per ordinamento, se tale clausola sia ammissibile con riferimento ai doveri deontologici, e al rischio di perdita dell'*attorney-client privilege*[11]. Comunque sia, tale uso richiede

[10] Per "*subpoena*", vedi definizione alla nota 9, *supra*. "Warrant" è un'autorizzazione, emessa da un giudice ovvero da un ufficiale governativo, diretta alla polizia o ad altro ente affinché si possano compiere arresti, perquisizioni ovvero altre azioni finalizzate all'amministrazione della giustizia.

[11] L'*attorney-client privilege* è un concetto tipicamente americano: il "privilegio" consente di escludere dalla *pre-trial discovery* le comunicazioni confidenziali tra avvocato (o suo procuratore) e cliente (o suo procuratore) effettuate per richiedere o prestare assistenza legale.

sempre il consenso, a meno che l'utilizzo da parte del *provider* non sia volto a compiere un'attività utile all'espletamento dell'incarico professionale (si pensi, per esempio, a quei SaaS che, al caricamento delle ore di lavoro, generano automaticamente la relativa parcella.)
- Cosa prevede contratto di *cloud* riguardo all'interruzione del servizio di *cloud* per manutenzione?
- Cosa prevede il contratto di *cloud* riguardo all'accesso ai dati e al ripristino dei dati nel caso in cui il servizio del *provider* sia interrotto temporaneamente o definitivamente?
- Quali metodi di *backup* utilizza il *provider*?
- Lo studio legale ha previsto un metodo di *backup* e recupero dei dati se questi non possano ottenersi dal *provider*?
- Dove si trovano i *server* del *cloud provider*? Nel caso in cui i *server* siano localizzati in paesi nei quali la legge privacy differisce da quella del luogo dove lo studio legale è ubicato, quale è la legge applicabile al trattamento dei dati? Quella straniera? Nel caso in cui si debba applicare la legge di straniera, e lo studio legale non voglia (o non possa) consentire che ai suoi dati si applichi quella legge, c'è qualcosa che lo studio legale o il *provider* possono fare per evitare di conservare i dati in quel paese?
- Cosa prevede contratto di *cloud* con riferimento alla restituzione dei dati al termine del servizio?
- Lo studio legale ha adottato procedure e criteri appropriati, ivi inclusa la formazione del proprio personale, riguardo all'utilizzo del *cloud* e dei dispositivi elettronici per accedervi?

Queste domande possono essere sintetizzate in una breve raccomandazione che considera i rischi interni ed esterni: nel decidere se utilizzare un servizio di *cloud*, uno studio legale dovrebbe verificare l'affidabilità del *cloud provider*, controllare che il contratto di *cloud* sia compatibile con le obbligazioni deontologiche (di competenza, confidenzialità, protezione della titolarità dei dati, supervisione di collaboratori e nelle comunicazioni col cliente), e con la legge privacy a cui lo studio è soggetto, oltre a stabilire procedure e criteri interni per l'utilizzo della *cloud* che ottemperino ai doveri professionali.

4. Fase della decisione

Lo studio legale deve decidere se utilizzare il servizio sulla base dell'analisi costi/benefici, dell'identificazione dei rischi, e delle misure che può adottare per minimizzare tali rischi. La decisione è in parte oggettiva e basata su costi e

Sul punto, vedi N.M. Crystal - F. Giannoni-Crystal, *Understanding Akzo Nobel: A Comparison of the Status of In-House Counsel, the Scope of the Attorney-Client Privilege, and Discovery in the U.S. and Europe*, in *Global Jurist*, 11-1 (Topics), Article 1, available at: http://www.bepress.com/gj/vol11/iss1/art1

benefici direttamente identificabili e in parte soggettiva, in quanto, da un lato non sarà sempre possibile quantificare gli eventuali benefici (come, per esempio, un aumento di produttività) e dall'altro, la possibilità che un certo rischio si concretizzi e le conseguenze per studio e clienti sono difficili da stimare.

5. Fase successiva alla decisione

L'analisi che lo studio legale deve compiere non deve fermarsi qui. La tecnologia utilizzata e la legge applicabile sono in continua evoluzione e gli avvocati sono chiamati ad essere sempre informati su tali cambiamenti. Di fatto, lo studio legale dovrebbe (i) rivedere periodicamente le misure adottate per la protezione dei dati personali; (ii) informarsi sulla *best practice* per la protezione dei dati personali e implementarla; e (iii) tenersi al passo con l'evoluzione della legge applicabile (in tutte le giurisdizioni in cui esso opera), specialmente (per gli avvocati americani) in tema di *attorney-client privilege*.