Presentazione

Luiss Law Review inizia con questo numero la pubblicazione di sezioni monografiche dedicate a temi di particolare rilievo da approfondire con prospettive e su aspetti diversi.

L'inserimento di una parte monografica non esclude in genere, come in questo numero, la presenza di altri contributi, così da lasciare spazio anche a sollecitazioni e analisi su argomenti diversi.

Questo primo dossier è dedicato a due materie oggi fondamentali, vicine e spesso interconnesse: la sicurezza informatica e la protezione della *Privacy* digitale nell'epoca, ormai a tutti gli effetti iniziata, dell'intelligenza artificiale.

Gran parte dei contributi trovano origine nel dottorato Diritto e Impresa del Dipartimento di Giurisprudenza Luiss Guido Carli diretto da Giuseppe Melis, grazie soprattutto all'impegno e alla passione di Riccardo Piselli, dottorando del XXXII ciclo.

Con riguardo alla Cyber Security, è indispensabile per il nostro Paese poter contare su una pubblica amministrazione consapevole delle minacce informatiche e in grado di difendersi adeguatamente. Come sottolinea il contributo di Marta Zilianti, negli ultimi anni sono stati fatti passi avanti importanti in questa direzione nonostante la limitatezza delle risorse economiche disponibili, che ne rappresenta forse il principale ostacolo. Si è in particolare proceduto a una nuova organizzazione della nostra struttura istituzionale di sicurezza informatica, rafforzando il coordinamento degli interventi di prevenzione, protezione e gestione affidato al CISR (Comitato interministeriale per la sicurezza della Repubblica) e al DIS (Dipartimento per l'informazione per la sicurezza).

Sul fronte delle imprese, specie minori, per elevare il livello di sicurezza informatica è auspicabile ricorrere anche a strumenti di collaborazione imprenditoriale quali il consorzio o il contratto di rete, ferma la necessità di un intervento anzi tutto pubblico in tema di *Information Sharing*, secondo le previsioni della Direttiva NIS. Strumenti che possono consentire di contenere i costi e di mettere in moto il percorso virtuoso ipotizzato dal Rapporto 2016 del

CIS e del Laboratorio nazionale di Cybersecurity, come osserva Gian Domenico Mosco. Possono contribuire anche strumenti agevolativi di carattere fiscale, pur di portata più ampia, come il c.d. iperammortamento esaminato nel contributo di Alessandro Liotta.

Problemi di sicurezza informatica e di protezione dei dati personali emergono anche quando si ricorre per la conclusione dei contratti e in genere per la sottoscrizione di documenti alla firma grafometrica, che consiste in una sottoscrizione elettronica ma olografa apposta su un tablet o su altri dispositivi, che possono rilevare anche dati biometrici identificativi del sottoscrittore quali la pressione o la velocità di tracciamento. Mentre già si intravedono gli ancora più ampi rischi della diffusione per l'identificazione di una persona della biometria fisica (iride, impronta digitale, volto, ecc.) o dei microchips sottopelle (secondo il *Wall Street Yournal,* già utilizzati nel mondo da non meno di 30.000 persone), emerge la necessità, messa in luce dal contributo di Maria Rosaria Lenti, di una forte attenzione verso il fenomeno, pur regolato da un provvedimento del 2014 dell'Autorità garante per la protezione dei dati personali, così da rendere più efficaci le misure di prevenzione e da poter reagire prontamente a minacce oggi ancora sconosciute o sottovalutate, ma probabili considerati la complessità del mondo digitale e lo sviluppo ancora iniziale dello strumento.

È inutile sottolineare l'importanza del diritto penale con riguardo alla Cyber Security, pur se attualmente non esiste una regolamentazione penalistica specifica della materia. Nel contributo di Luca D'Agostino si osserva però che il recepimento della direttiva NIS - 2016/1148 UE e in parte le stesse fonti di auto-regolamentazione comporteranno, almeno per i fornitori di servizi essenziali o di servizi digitali, obblighi di *compliance* e una conseguente responsabilità in caso di mancata o insufficiente adozione di misure adeguate di prevenzione e protezione o di violazione degli obblighi di notifica, con un presumibile rafforzamento dei presidi organizzativi per la sicurezza informatica.

A livello europeo, è l'ENISA, l'Agenzia Europea per la sicurezza delle reti e dell'informazione creata nel 2004, a occuparsi della materia: il contributo di

Elena Pauri ricostruisce l'attuale quadro normativo ed esamina le prospettive di riforma dell'Agenzia.

Vantaggi e pericoli dell'intelligenza artificiale, e dei Big Data che ne sono alla base, sono divenuti oggetto di dibattito anche non specialistico via via che se ne è toccata con mano la diffusione nella vita di tutti i giorni, una diffusione senza dubbio destinata a incrementarsi fortemente, ma con contenuti (se e quando la I.A. assomiglierà a quella umana?) oggi non prevedibili sulla base delle tecnologie disponibili. Come si sta cercando di governare l'Intelligenza Artificiale e cosa andrà fatto in futuro è indicato nella ricca ricognizione di Tulio Rosembuj.

Uno dei problemi più rilevanti suscitati dall'I.A. è senza dubbio la tutela della *Privacy,* ormai vista essenzialmente come protezione dei dati personali.

Non è un caso che il Regolamento (UE) 2016/679 in materia di protezione di dati personali preveda che dal 25 maggio 2018 vi siano limiti al trattamento dei dati personali che avvenga sulla base di un processo decisionale "automatizzato" e che, se il trattamento è consentito, l'interessato abbia almeno il diritto di ottenere l'intervento umano del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. Altrettanto significativo è che chiunque di noi abbia dal prossimo maggio il c.d. "diritto alla spiegazione", vale a dire il diritto di ricevere "informazioni significative", tra l'altro, sulla "logica utilizzata" dall'algoritmo.

Riccardo Piselli si interroga però sui limiti del regolamento 2016/679 di fronte allo sviluppo degli algoritmi di *deep learning* e sulla *privacy* come strumento che ormai si affianca al diritto *antitrust* nella regolamentazione della competizione imprenditoriale, mentre il diritto alla portabilità dei dati anche come fattore pro-concorrenziale è esaminato nel contributo di Andrea Giulia Monteleone.

Infine, Ernani Francesco Cesareo si occupa dell'introduzione da parte dell'art. 24 del regolamento (UE) 2016/679 del principio di *Accountability,* che chiama il responsabile del trattamento a mettere in atto misure tecniche e

organizzative adeguate per garantire che il trattamento sia realizzato nel rispetto del regolamento e a poterlo dimostrare.

L'importanza e la complessità dei problemi suscitati dall'Intelligenza Artificiale è testimoniata dall'approvazione da parte del Parlamento europeo il 16 febbraio 2017 di una risoluzione che raccomanda alla Commissione di predisporre una regolamentazione civilistica della robotica e di valutare l'opportunità di istituire un'Agenzia europea per la robotica e l'intelligenza artificiale. Avremo presto una direttiva europea in materia, speriamo organica e ben meditata?