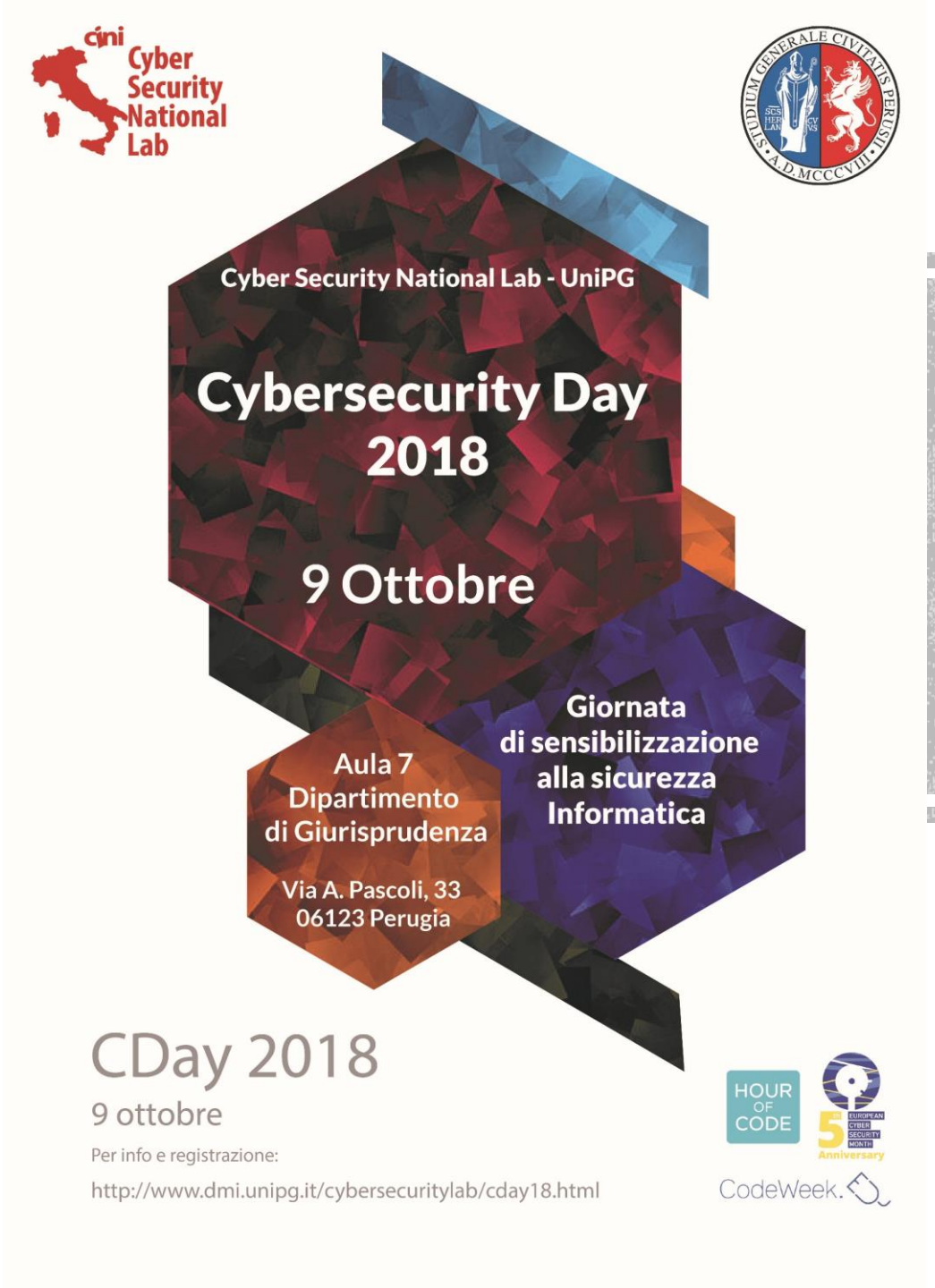

Il Libro Bianco CINI Cybersecurity "Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici". Apporti del nodo UniPG

Prof.ssa Stefania Stefanelli
Università degli studi di Perugia

ART. 82 GDPR: DIRITTO AL RISARCIMENTO E RESPONSABILITÀ

- 1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
- 2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
- 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

ART. 82 GDPR: DIRITTO AL RISARCIMENTO E RESPONSABILITÀ

- 4. (solidarietà) Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
- 5. (diritto di regresso) Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.
- 6 (giurisdizione nazionale) Stato di stabilimento del titolare o del responsabile, o in alternativa quello in cui l'interessato stabilmente risiede, salvo che l'azione sia promossa contro un'autorità pubblica dello Stato, nell'esercizio dei suoi poteri

CONSIDERANDO

- 74 «È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche»
- 146 «Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile»

ART. 24 GDPR: RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

ART. 15, COMMA 2, D.LGS. 196/2003

Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 (*Modalità del trattamento e requisiti dei dati)*

ART. 2050 C.C.

- **Responsabilità per l'esercizio di attività pericolose.**

Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno

Regola più rigorosa di quella dell'art. 2043 c.c. (che obbliga il danneggiato a provare, oltre il fatto illecito, il danno ingiusto e il nesso di causalità tra gli stessi, anche il dolo o la colpa del danneggiante)

Attività «caratterizzata da notevole potenzialità di danno, da una pericolosità intrinseca o comunque dipendente dalle modalità di esercizio e dai mezzi di lavoro impiegati» (Cass. 8304/1987)

ART. 2050 C.C.

- È la responsabilità dell'organizzatore dell'attività sportiva, riferita alla natura dei mezzi adoperati
- Cass. 8457/2004: fattispecie di responsabilità oggettiva, che prescinde dalla colpa del responsabile (Trimarchi), ovvero di presunzione di responsabilità

ART. 2054 C.C.

- Il conducente di un veicolo senza guida di rotaie è obbligato a risarcire il danno prodotto a persone o a cose dalla circolazione del veicolo, se non prova di aver fatto tutto il possibile per evitare il danno

- La circolazione dei veicoli è una delle attività pericolose tipiche, come lo era il trattamento dei dati personali, e lo è ancora la responsabilità da prodotto difettoso

ORIENTAMENTI GIURISPRUDENZIALI

- Rispondere esige pur sempre un criterio di imputazione (altrimenti si tratterebbe di garanzia), e nell'art. 2050 c.c. questo criterio, alternativo alla colpa, è la pericolosità, che fonda un'inversione dell'onere della prova
- Non è il danneggiato a dover provare la colpa del danneggiante, ma è costui a dover dimostrare l'adozione di tutte le misure idonee ad evitare il danno
- La prova liberatoria non verte sulle modalità di causazione del danno, ma sulle modalità di organizzazione dell'attività, che devono apparire idonee a prevenire l'eventualità di eventi dannosi
- L'attività pericolosa deve essere svolta nelle condizioni di massima sicurezza, con l'adozione di tutti gli accorgimenti che la tecnica offre; se ciò nonostante il danno si è verificato, sarà un evento inevitabile, non imputabile, ovvero non in rapporto di causalità con lo svolgimento dell'attività

PROVA LIBERATORIA

- Prova critica (non storica)
- Soddisfatta anche quando restino ignote le cause che hanno prodotto il danno (Cass. 10382/2002)
- Quando la tecnica non possa garantire la prevenzione di danni, la prova liberatoria è fornita provando di aver adottato tutte le misure allo stato offerte dalla tecnica, anche se non ancora del tutto idonee a scongiurare eventi dannosi
- Cass. 10638/2016: In tema di ripartizione dell'onere della prova, al correntista abilitato a svolgere operazioni "on line" che … agisca per l'abusiva utilizzazione (nella specie, mediante illegittime disposizioni di bonifico) delle sue credenziali informatiche, spetta soltanto la prova del danno siccome riferibile al trattamento del suo dato personale, mentre l'istituto creditizio risponde, quale titolare del trattamento di dati, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico mediante la captazione dei codici d'accesso del correntista, ove non dimostri che l'evento dannoso non gli sia imputabile perché discendente da trascuratezza, errore o frode del correntista o da forza maggiore

NIENTE DI NUOVO SOTTO IL GDPR

- Art. 82, § 3: Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile
- Art. 24, § 1: Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

ANZI, QUALCOSA DI ANTICO

- Art. 24, § 3: L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento
- Codice adottato da CISPE.cloud per gli operatori che offrono servizi di cloud computing https://cispe.cloud/code-of-conduct/
- Linee guida Confindustria danese https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen_engelsk.pdf

LIBRO BIANCO 2018 CINI

- Si sta delineando un'evoluzione verso il cosiddetto *Next Generation SOC*, nel quale un ruolo determinante è svolto da strumenti di *soft law* e fonti di autoregolamentazione di categoria, attraverso regole di correlazione che includono metodi e tecniche di analisi business oriented e, soprattutto, sono integrabili con strumenti di monitoraggio predisposti per i Big Data.

Security Operations Center (SOC) – Centro per la fornitura di servizi finalizzati alla sicurezza dei sistemi informativi interni a un'azienda o di clienti esterni. Le tipologie di servizi offerti tipicamente includono: (i) gestione delle funzionalità di sicurezza legate all'infrastruttura IT (rete, sistemi e applicazioni); (ii) monitoraggio dell'infrastruttura IT per individuare tempestivamente tentativi di intrusione o uso improprio dei sistemi; (iii) controllo per migliorare il livello di protezione attraverso *security assessment* ed *early warning*. Pur avendo ruoli e finalità tra loro diversi, in alcuni casi i SOC fungono anche da CERT (si veda il box a pag. 20).

CODICI DI CONDOTTA IN ATTESA DI APPROVAZIONE

- Assintel: Codice di Condotta per le aziende ICT
- Federprivacy
- Sanità: Codice di Condotta promosso da Aitems; bozza di codice di condotta per le applicazioni mobili nel settore della salute, promosso dalla Commissione europea (su cui ha espresso parere l'Art.29 *Working Party*, col GDPR sostituito da *European Data Protection Board* - Comitato europeo per la protezione dei dati, composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti)
- Banche centrali sovranazionali (MENA - *Middle East & North Africa*, AFRICA, ECA - *Europe & Central Asia*) e Banca mondiale/IFC (WBG – *World bank group*): centrali rischi e delle informazioni commerciali

Sicurezza nell'interazione Umani- Robot in ambienti sociali

Sicurezza, ma anche resilienza e safety, in particolare in ambienti domestici e camere operatorie

MOTIVAZIONE

- Trasformazione degli aspetti quotidiani e lavorativi della vita umana.
- Aumento dell'esposizione dell'uomo al contatto con le macchine e con i pericoli che se ne ingenerano.
- Progressivo sviluppo di meccanismi intelligenti ed autonomi, capaci di prendere decisioni indipendenti.
- Esigenza di avere un quadro dell'insieme delle esternalità negative prodotte dall'impatto dell'IA con la realtà umana, individuale e collettiva.
- Regolamentazione degli aspetti etici, medici, sociali, giuridici di questi nuovi contesti relazionali.

Stato dell'arte in Italia, in Europa, nel mondo relativamente a progetti (o programmi di progetti) similari

- Nel 2016 viene approvato un documento di studio sulle regole giuridiche civili europee in materia di robotica.

- Principi etici:

✓ Dovere per i robot di non causare offese agli individui umani
✓ Rispetto delle regole di cautela ed attenzione nei confronti dell'uomo
✓ Responsabilità civile oggettiva per i danni causati dai robot

- Dal gennaio 2017 è allo studio della Commissione Affari legali dell'UE la formulazione di una proposta di direttiva europea sulle regole civilistiche della robotica.

.

Sfide di ricerca, di innovazione e di progresso tecnologico

- Profili di criticità:

✓ gestione/manipolazione dei dati personali dell'individuo acquisiti dal robot nei contatti sociali;

✓ manipolazione delle emozioni umane dei soggetti deboli in contatto quotidiano con macchine artificiali sociali (robot in ambienti domestici o paradomestici, vicini ad anziani, bambini, malati);

✓ vulnerabilità fisica di chi usa apparecchi meccanici sanitari per integrare/sostituire proprie disfunzionalità organiche.

- Metodo per affrontare lo specifico rischio: raccogliere in via precauzionale gli indizi sintomatici del percorso degenerativo, per impedirne l'evoluzione o magari per consentirne la reversibilità.

- Definizione scritta ed uniforme, in via convenzionale "internazionale", delle nuove regole cautelari che sorgono al contatto dell'uomo con macchine artificiali

- Sviluppo della fase dei test delle attività robotiche in scenari di vita-reale

Obiettivi pratici del progetto

- In ambito medico-chirurgico:

✓ supportare la chirurgia in forma meno invasiva
✓ implementare l'esperienza umana di diagnosi e trattamento delle patologie fisiche e psichiche
✓ mantenere l'umanità del rapporto collaborativo tra medico e paziente;
✓ salvaguardare la salute del paziente e ridurre il rischio medico

- Condividere un sistema di imputazione della responsabilità per danni prodotti da macchine automatizzate o autonome, nei vari campi di rispettivo utilizzo.

- Sistema di garanzie:

✓ per un controllato consenso dell'uomo ad entrare in contatto con il robot
✓ per la non personale identificabilità, da parte della macchina, del singolo suo utente

Ruolo nel progetto di:
1. Università ed Enti Ricerca

Coordinamento per monitoraggio ed aggiornamento dei risultati della ricerca in materia di robotica e di macchine artificiali. Verifica dello stato della regolamentazione vigente in materia.

2. Aziende
(possibile divisione tra grandi, medie, piccole)

Verifica dello stato di utilizzo e produzione di macchine artificiali e prodotti della robotica; verifica dell'esperienza lavorativa (le tecnologie di sicurezza dei lavoratori nella produzione del sistema artificiale; la dotazione del sistema artificiale con apparecchiature di protezione dell'utente).

3. Governo e PA

Finanziamento della ricerca, in mezzi e risorse (umane e strutturali)

Ricadute del progetto su:

- Società, per instaurare e sviluppare relazioni sociali – uomo/robot – nel rispetto della dignità umana.
- Industria, per ottimizzare la sicurezza nella lavorazione del prodotto e nell'uso del prodotto finito.
- Ricerca, per progredire nella cognizione della robotica al servizio dei bisogni umani.
- Paese, per la formazione di un articolato ed equilibrato sistema etico e di responsabilità giuridica