MODULO PRESENTAZIONE PROPOSTE PROGETTUALI

Acronimo: LIC (Law in Cyberspace)

Titolo: Cyberspazio e diritto: strumenti giuridici per la tutela dal rischio cibernetico

Riassunto: (*massimo 3000 caratteri spazi esclusi*)
La ricerca ha ad oggetto il ruolo ascrivibile al diritto, quale strumento di *policy* funzionale alla tutela di interessi individuali e collettivi, nel contesto fenomenico del cyberspazio.
L'idea di potersi liberare da vincoli e rigidità, fondata sull'aspettativa di autonomia delle basi tecniche e dei *software* di *internet*, che, negli auspici, avrebbero consentito lo sviluppo di negoziazioni e di comportamenti *on-line* al di là di qualunque intervento regolatore, si è rivelata infatti, ben presto, una mera illusione. Il rischio correlato alla minaccia digitale, atteso l'elevato numero degli utenti "attaccati" e i conseguenti ingenti pregiudizi, che interessano trasversalmente la sfera dei diritti individuali e si proiettano su quella collettiva, ha assunto proporzioni a dir poco allarmanti, collocando la materia della *cybersecurity*, anche per le ricadute sul piano della sicurezza nazionale, tra le prioritarie esigenze presenti nelle agende politiche. Ciò è testimoniato dalla continua produzione normativa, che, risalente già alla fine del secolo scorso (cfr. l. 23 dicembre 1993 n. 547, con cui sono state introdotte le principali figure di reato informatico, successivamente riformulate e ampliate) e prevalentemente di derivazione internazionale (cfr. Raccomandazione del 1989 del Consiglio d'Europa sulla necessità di contrastare i reati informatici, seguita nel 2001 dalla stipulazione, da parte degli Stati membri del Consiglio, della Convenzione di Budapest sul *cybercrime*, in attuazione della quale si è assistito all'inclusione dei reati informatici nel catalogo dei reati presupposto della responsabilità dell'ente *ex* d.lgs.231/2001), si è resa particolarmente fitta negli ultimi anni. Limitandoci agli atti principali e più recenti, si possono menzionare: il d.lgs. n. 65 del 2018 di attuazione della Direttiva UE 2016/1148 recante «Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione»; il d.l. n. 105 del 2019, col quale si è istituito il Perimetro di sicurezza nazionale cibernetica; il *Cybersecurity Act* (Regolamento UE 2019/881), volto a istituire un meccanismo di certificazione in materia e a rafforzare il ruolo dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA); il d.l. n.82 del 2021, che ha istituito la nuova Agenzia per la Cybersicurezza Nazionale (ACN), attribuendole compiti di vigilanza, potestà ispettive e sanzionatorie; il *Digital Service Act* (Regolamento UE 2022/2065), di contrasto alla disinformazione *on-line*; il *Digital Operational Resilience Act* (Regolamento UE 2022/2054), per la tutela del settore finanziario; oltre alla Direttiva UE 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, e alla Direttiva UE 2022/2557, in materia di servizi essenziali, da recepire entrambe entro il 17 ottobre 2024.
In questo complesso e variegato quadro, il progetto, indirizzando il *focus* sul tema delle tutele giuridiche attraverso un approccio multidisciplinare, si propone di vagliare e individuare strumenti esegetici, buone prassi procedurali ed eventuali soluzioni normative a garanzia di un adeguato livello di protezione degli interessi coinvolti.

Parole chiave (*massimo 5*)**:**
cybersecurity, *cyberattack*, diritti, *compliance*

Nome del Responsabile Scientifico:
Andrea Francesco Tripodi

Elenco dei partecipanti:

Nome del partecipante	Qualifica	Dipartimento/ Istituzione	SSD
Andrea Francesco Tripodi	*Professore associato*	*Dipartimento di Giurisprudenza*	*IUS17 12-Scienze giuridiche 12/G1- Diritto penale*
Ermanno Calzolaio	*Professore ordinario*	*Dipartimento di Giurisprudenza*	*IUS 02 12-Scienze giuridiche 12/E2-Diritto privato comparato*
Claudia Cesari	*Professore ordinario*	*Dipartimento di Giurisprudenza*	*IUS16 12-Scienze giuridiche 12/G2-Diritto processuale penale*
Fabrizio Marongiu	*Professore ordinario*	*Dipartimento di Giurisprudenza*	*IUS13 12-Scienze giuridiche 12/E1-Diritto internazonale*
Carlo Piergallini	*Professore ordinario*	*Dipartimento di Giurisprudenza*	*IUS17 12-Scienze giuridiche 12/G1-Diritto penale*
Roberto Acquaroli	*Ricercatore*	*Dipartimento di Giurisprudenza*	*IUS17 12-Scienze giuridiche 12/G1-Diritto penale*
Laura Bartoli	Ricercatore T.D. art. 24 c.3-a L. 240/10	*Dipartimento di giurisprudenza* Università di Bologna	*IUS16 12-Scienze giuridiche 12/G2-Diritto processuale penale*
Paolo Sernani	Ricercatore T.D. art. 24 c.3-b L. 240/10	*Dipartimento di giurisprudenza*	*ING-INF/05 09-Ingegneria industriale e dell'informazione 09/H1- Sistemi di elaborazione delle informazioni*
Sirio Zolea	Ricercatore T.D. art. 24 c.3-b L. 240/10	*Dipartimento di giurisprudenza* Università Roma Tre	*IUS 02 12-scienze giuridiche 12/E2-Diritto privato comparato*
Karine Bannelier	Senior lecturer	Université de Grenoble-Alpes	IUS 13 *International law*

Piano finanziario stimato

Tipologia di spesa	Importo in Euro	Descrizione

Invito di esperti e relatori	2000	Spese di viaggio e soggiorno esperti e relatori per convegni e seminari
Pubblicazioni	2000	Volume Atti del convegno
Trasferte (trasporto e soggiorno)	1000	Spese di trasferta per reperimento dati e ricerca
Partecipazione a / organizzazione di eventi (conferenze, seminari, ecc.)	5000	Organizzazione convegni finali
Altro (da specificare)		
TOTALE 10000		

Indice

1: Qualità scientifica e/o tecnica

1.1 Idea e obiettivi (massimo 5000 caratteri, spazi bianchi esclusi)

Spiegare l'idea del progetto. Quali sono le principali idee che hanno portato a proporre questo progetto? Descrivere in dettaglio gli obiettivi scientifici. Gli obiettivi devono essere raggiungibili in seno al progetto, non attraverso un ulteriore e successivo sviluppo. Essi debbono essere misurabili e verificabili.

La centralità assunta dal cyberspazio nel contesto sociale, a cui si accompagna il tipico rischio da innovazione tecnologica, impone di ripensare in maniera profonda il tema delle tutele giuridiche.
Le stime dell'*European Cyber Center* e dell'Associazione italiana per la sicurezza informatica consentono di conferire rilievo macroeconomico alle perdite dovute agli attacchi informatici. I pregiudizi correlati al fenomeno della minaccia digitale sono ancor prima apprezzabili nella prospettiva del diritto emergente alla *riservatezza informatica tout court*, definibile come *diritto a uno spazio informatico libero da atti di incursione di soggetti terzi*, funzionale alla piena affermazione della persona nella moderna società dei rapporti comunicativi. Strumentale alla protezione degli interessi raggiunti dalle ricadute negative del fenomeno cibernetico, è dunque il bene, anch'esso in via di inquadramento, della *sicurezza informatica*, che assume rilievo pubblicistico, pure in chiave di sicurezza nazionale, quando apprezzato con riferimento ai settori dei servizi essenziali e delle infrastrutture critiche, e, più in generale, dei sistemi in dotazione della P.A.
Il tratto di vulnerabilità che connota la posizione dell'utente della rete – *status* che presenta caratteri di universalità, non essendo circoscrivibile all'area dei soggetti tradizionalmente qualificati dal lessico giuridico come deboli – reclama una revisione dell'intero ordinamento giuridico, che sappia coniugare le esigenze tutelari con quelle connesse ai traffici economici e alle dinamiche informative; una revisione evidentemente già in atto, come testimoniato dalla frenetica evoluzione normativa di prevalente origine *internazionale.*
Nell'ottica *penalistica*, alla varietà dei beni giuridici interessati dal risvolto patologico del fenomeno corrisponde l'ampiezza concettuale della categoria del *cybercrime*, il cui carattere accomunante risulta essere il contesto stesso dell'operatività criminale, ossia il *cyberspace*, con una conseguente trasversalità delle aree attratte nel campo d'analisi (reati informatici, in materia di *privacy*, in materia di terrorismo, contro la persona, di riciclaggio, di violazione del diritto d'autore, del mercato finanziario, etc.). Occorrerà allora vagliare, anche in chiave di *dimostrazione probatoria*, la tenuta delle attuali fattispecie di reato e degli strumenti investigativi tradizionali al cospetto delle più recenti manifestazioni degli attacchi digitali e, correlativamente, la capacità di resistenza delle categorie classiche della tipicità penale – azione, causalità, evento – pure alla luce dell'uso in ambito cibernetico di strumenti dell'i*ntelligenza artificiale*, così da poter conclusivamente pervenire all'eventuale elaborazione di una proposta riformatrice. Parallelamente, si terrà conto dell'aspetto più rilevante dell'*enforcement* normativo in materia, che non si ravvisa tanto sul piano tradizionale del diritto penale cd. "reattivo", ossia orientato a reagire alle conseguenze attraverso la previsione di figure incriminatrici, quanto sul piano, affermatosi in tempi più recenti, del diritto punitivo "proattivo", ossia orientato a prevenire l'illecito penale mediante l'imposizione di obblighi – o la previsione di facoltà – di *compliance*, la cui violazione determina l'irrogazione di sanzioni amministrative a carico dell'ente, soggette il più delle volte, per le loro caratteristiche, allo statuto penale. Su questo versante, per via dell'ausilio

determinante del sapere tecnico *ingegneristico*, saranno oggetto di ricognizione, con l'obiettivo di fornire un contributo migliorativo ovvero di individuare una sorta di procedura prevenzionistica "pilota", sia le procedure aziendali implementate in funzione di ridurre il rischio di commissione di *cybercrimes* all'interno dell'ente – si pensi alla captazione abusiva di flussi comunicativi, alla manipolazione di dati posta in essere nell'interazione con la P.A., alle condotte di danneggiamento del funzionamento di sistemi informatici e telematici altrui – sia quelle prospettate in chiave difensiva dagli attacchi esterni. In quest'ultimo ambito sono stati imposti alle imprese e alle P.A., che operano in settori di interesse strategico per lo Stato o fondamentali per il vivere civile, penetranti obblighi di *compliance*, tra i quali l'adozione di particolari misure di sicurezza e la notifica di incidenti. Ulteriori obblighi di *compliance* riguardano poi gli *Internet service providers* e in particolare i gestori delle grandi piattaforme *online*, che agiscono come *gatekeepers* per evitare la diffusione di informazioni false o di contenuti illegali.
Nell'ottica *privatistica*, si pone l'esigenza di identificare forme di tutela per i titolari delle nuove entità immesse e fatte circolare nella rete, quando ad esempio esse finiscono per disperdersi in essa a causa di interventi fraudolenti. Sono già numerosi i casi in cui, in ogni ordinamento, i giudici si trovano a doversi confrontare con dati, criptovalute, NFT, in un contesto caratterizzato dalla scarsità (se non proprio dall'assenza) di norme legislative. Occorrerà, allora, preliminarmente interrogarsi sulla natura giuridica dei beni che circolano in rete, adottando un approccio comparatistico, attesa la natura globale dei fenomeni implicati, per poi analizzare la relazione tra istituti tradizionali – quali, ad esempio, la responsabilità contrattuale ed extracontrattuale – e i rapporti giuridici nati nel *cyberspace,* al fine di individuare possibili forme di reintegrazione patrimoniale e, più in generale, di tutela privatistica dai potenziali pregiudizi subiti dalle persone fisiche e giuridiche a seguito di un *cyberattack*.

1.2 Progresso dello stato dell'arte (massimo 5000 caratteri, spazi bianchi esclusi)
Descrivere lo stato dell'arte nel settore di ricerca cui il progetto si riferisce e il progresso cui la proposta progettuale condurrebbe.

La scienza penalistica ha manifestato piena consapevolezza delle problematiche poste dai *cybercrimes*, evidenziando come alcune categorie concettuali plasmate sull'agire umano *in rerum natura* – in particolare gli elementi del fatto tipico e dunque le stesse modalità d'offesa – assumano nel cyberspazio connotati del tutto peculiari, così da richiedere un intervento di riadattamento intepretativo coerente con la realtà virtuale e non più fisica, nella quale si consuma il reato (si pensi, a titolo d'esempio, alla problematica individuazione del *locus commissi delicti*, atteso peraltro il carattere transnazionale del fenomeno). Correlativamente, in ambito processuale, si è assistito a un sostanzioso, ma ancora insufficiente aggiornamento delle categorie tradizionali (per esempio il sequestro, oggi esteso anche ai dati). Allo stesso tempo, il campo d'indagine si è smaterializzato ed ampliato, cosa che ha reso complesso il contesto operativo: da un lato, la collaborazione giudiziaria è sempre più importante nell'accertamento di reati di ogni tipo perché gli elementi di prova, pur prodotti in Italia, potrebbero essere custoditi ben oltre i confini nazionali; dall'altro, l'interconnessione dei sistemi rende difficile, se non impossibile, l'effettiva cattura degli indagati.
I tratti di complessità del quadro di riferimento si acuiscono allorquando ad operare nel contesto digitale sia un prodotto dell'intelligenza artificiale di ultima generazione (si pensi, a titolo d'esempio, agli *High Frequency Traders*, programmi informatici basati su complessi

strumenti algoritmici, a cui è affidato il compimento di operazioni nei mercati finanziari), rispetto al quale il distacco della macchina dalla componente umana rende particolarmente disagevole l'itinerario di ascrizione della responsabilità che risale, secondo modelli imputativi classici, all'uomo, lasciando invece prefiguare scenari avveniristici a dir poco arditi (come quello, già prospettato nella letteratura straniera, del sistema penale dei robot).
In questa prospettiva, all'esito di una ricognizione dell'assetto giurisprudenziale e dottrinale, si tenterà di proporre soluzioni interpretative rispettose dei principi penalistici, senza mancare di fornire indicazioni nella direzione della progettualistica riformatrice.
Nella complementare prospettiva del diritto penale "proattivo", è dato rinvenire, nella struttura organizzativa degli enti, l'implementazione di procedure preventive dei *cybercrimes* in continua evoluzione, attesa la mutevolezza delle tecniche di attacco, le quali si sviluppano di pari passo con i nuovi ritrovati tecnologici. Il tentativo di rendere un contributo in termini di affinamento delle prassi procedurali, avvalendosi anche dell'*expertise* ingegneristica coinvolta nel progetto, non potrà prescindere dalla previa analisi delle stesse, anche attraverso il coinvolgimento delle associazioni di categoria.
Nell'ottica privatistica, data la mole di attività compiute nel *cyberspace* e le crescenti minacce cibernetiche che si verificano a livello internazionale, emerge una sempre maggiore vulnerabilità dei soggetti giuridici che possono subire pregiudizi patrimoniali. Attualmente, tuttavia, non è prevista una specifica disciplina normativa nazionale all'avanguardia sul tema, né è possibile registrare un'adeguata attenzione da parte della dottrina relativamente alle necessarie forme di reintegrazione patrimoniale cui ricorrere nel caso di danni subiti dalle persone fisiche e giuridiche a seguito di *cyberattacks*. In presenza di quelle dinamiche patologiche del rapporto privato che possono verificarsi ad esito di un *cyber risk* concretizzato, occorrerà allora soffermarsi, in particolare, sull'applicabilità di istituti quali la responsabilità contrattuale e extracontrattuale, la ripetizione dell'indebito e l'ingiustificato arricchimento, arrivando a prospettare, sulla base di un approfondimento comparatistico, reso necessario dalla transnazionalità del fenomeno, soluzioni esegetiche ovvero indicazioni circa un futuro intervento normativo.
Infine, la stessa dimensione transnazionale del fenomeno, avvertita a livello dell'Unione Europea e più in generale in sede internazionale, spiega l'esigenza di armonizzazione delle legislazioni nazionali, rendendo dunque le relative fonti un necessario parametro di adeguamento delle opzioni normative interne e lo stesso diritto internazionale un osservatorio irrinunciabile dal quale guardare a tali sviluppi. Al contempo, la non rispondenza del cyberspazio a limiti geografici, impattando sullo stesso esercizio della sovranità dei singoli Paesi, tematizza in maniera problematica il fenomeno della cooperazione in una fase storica in cui le dinamiche di ordine geopolitico incidono, inevitabilmente, sul progredire di una regolamentazione coerente a livello internazionale di un settore tanto tecnico e complesso. La natura globale della fenomenica cyberspaziale spinge verso quantomai complesse intese, da raggiungersi in un contesto il più ampio possibile, cioè a vocazione universale, pur sempre disancorate da rigide ed anacronistiche visioni stataliste e opportunamente coordinate con i percorsi di armonizzazione già efficacemente tracciati.

1.3 Metodologia S/T e relativo piano di lavoro (massimo 10.000 caratteri)

Presentare un piano di lavoro dettagliato, suddiviso in attività che debbono seguire le fasi logiche di implementazione del progetto e includere la valutazione del progresso delle attività e dei risultati.

Presentare il piano di lavoro come segue:
i. Descrivere la strategia complessiva del piano di lavoro;

La strategia del piano di lavoro prevede come punto di partenza la rilevazione degli attuali livelli di tutela giuridica dagli attacchi digitali, a seconda dei vari interessi minacciati. L'analisi, declinata nella prospettiva penalistica "reattiva" e in quella privatistica, avrà come esito l'identificazione dei punti di criticità del sistema e l'elaborazione di proposte risolutive sul piano interpretativo e/o riformatore. La medesima strategia verrà adottata nell'ottica "proattiva" dunque con riferimento all'apparato procedurale costruito negli enti collettivi in funzione preventiva del *cybercrime* e di difesa dal medesimo, così da far emergere eventuali profili critici quanto al reale impatto in termini di prevenzione del reato e al pericolo di appesantimento delle dinamiche organizzative dell'ente. Tale indagine, che avrà corso durante la seconda annualità, si concluderà con l'elaborazione di soluzioni procedurali migliorative e con la promozione di una sorta di procedura "pilota" diversificata per settori di riferimento.

ii. Fornire una descrizione del lavoro, suddivisa in attività:

a) Analisi ricognitiva di legislazione, giurisprudenza e dottrina in materia di *cybercrimes* nella prospettiva delle tutele penalistiche e privatistiche, con individuazione di specifiche aree di criticità ritenute meritevoli di intervento ai fini dell'innalzamento del livello di tutela. 8 mesi
a.1) Riunione intermedia del gruppo di ricerca per analisi trasversale dei dati emersi dall'indagine ricognitiva. mese n.4
a.2) Riunione conclusiva del gruppo di ricerca finalizzata alla sistemazione delle aree di criticità individuate. mese n.8

b) Identificazione di soluzioni interpretative e/o elaborazione di proposte di riforma. 8 mesi
b.1) Riunione intermedia del gruppo di ricerca per analisi trasversale dei dati e selezione degli strumenti rimediali ritenuti praticabili. mese n.11
b.2) Riunione conclusiva del gruppo di ricerca finalizzata alla definitiva messa a punto degli strumenti rimediali selezionati mese n.14
b.3) organizzazione di un'iniziativa seminariale rivolta a dottorandi e studenti. mese n. 15
b.4) Organizzazione di un convegno interdisciplinare finale (anche con studiosi di aree scientifiche diverse dall'area 12) avente a oggetto le soluzioni elaborate. mese n.16

c) Analisi ricognitiva degli assetti procedurali implementati negli enti collettivi in funzione preventiva del *cybercrime* e a difesa dal medesimo, con individuazione di profili di criticità. 4 mesi
c.1) Riunione intermedia del gruppo di lavoro con esperti del settore, membri di funzioni aziendali e esponenti delle associazioni di categorie, funzionale all'emersione di profili di criticità procedurali. mese n.18
c.2) Riunione conclusiva del gruppo di ricerca finalizzata alla sistemazione delle aree di criticità procedurali. mese n.20

d) Proposta di interventi migliorativi sull'assetto procedurale e elaborazione di una procedura "pilota". 4 mesi
d.1) Riunione intermedia del gruppo di ricerca finalizzata alla selezione degli strumenti rimediali ritenuti praticabili. mese n.22

d.2) Riunione conclusiva del gruppo di ricerca finalizzata alla definitiva messa a punto degli strumenti rimediali selezionati. mese n.23
d.3) Organizzazione di un'iniziativa seminariale rivolta a dottorandi e studenti. mese n.23
d.4) Organizzazione di un convegno interdisciplinare finale (anche con studiosi di aree scientifiche diverse dall'area 12) avente a oggetto le soluzioni elaborate. mese n.24
d.5) Organizzazione di un'iniziativa di public engagement, *tramite incontro con le comunità locali*, *funzionale alla condivisione in chiave divulgativa dei benefici della ricerca nella prospettiva di educare i singoli (in specie, coloro che non possiedono competenze culturali idonee a comprendere il rischio-cyber e ad attivarsi di conseguenza in maniera tempestiva) alla difesa dai* cybercrimes*.* mese n.24

- *elenco delle attività (usare tabella 1.3a);*
- *descrizione di ogni attività (usare tabella 1.3b).*

Tabella 1.3 a: Elenco delle attività

Attività n.	**Titolo della attività**	**Ricercatori coinvolti**	**Coinvolgimento del Corso di dottorato in Diritto e Innovazione (indicare Si o No)**	**Mese di inizio**	**Mese di fine**
1	Analisi ricognitiva di legislazione, giurisprudenza e dottrina in materia di *cybercrimes* nella prospettiva delle tutele penalistiche e privatistiche, con individuazione di specifiche aree di criticità, ritenute meritevoli di intervento ai fini dell'innalzamento del livello di tutela.	Tripodi, Acquaroli, Calzolaio, Cesari, Marongiu, Piergallini, Bartoli, Zolea, Bannelier	No	1	8
2	Identificazione di soluzioni interpretative e/o elaborazione di proposte di riforma	Tripodi, Acquaroli, Calzolaio, Cesari, Marongiu, Piergallini, Bartoli, Sernani, Zolea, Bannelier	SI	9	16
3	Analisi ricognitiva degli assetti procedurali implementati negli enti collettivi in funzione preventiva del *cybercrime* e a difesa dal medesimo, con	Tripodi, Acquaroli, Piergallini, Sernani, Bannelier	No	17	20

	individuazione di profili di criticità.				
4	Proposta di interventi migliorativi sull'assetto procedurale e elaborazione di una procedura "pilota".	Tripodi, Acquaroli, Piergallini, Sernani, Bannelier	SI	21	24

Tabella 1.3 b: Descrizione delle attività

Per ogni attività:

Attività n.1

Obiettivi: Analisi ricognitiva e identificazione delle aree di criticità

Descrizione del lavoro e ruolo dei partecipanti: Tutti i ricercatori appartenenti all'area scientifica 12 (scienze giuridiche) saranno impegnati, per materia di competenza, anche in un'ottica comparatistica e con particolare attenzione alle fonti internazionali, nella raccolta dei dati legislativi, giurisprudenziali e dottrinali, così da identificare, in relazione alla tipologia di interessi tutelati, le aree caratterizzate da un basso livello di tutela giuridica. Si prevede una riunione del gruppo di ricerca intermedia, finalizzata all'analisi trasversale dei dati, e una conclusiva, finalizzata alla sistemazione dei risultati.

Attività n.2

Obiettivi: Proposte di soluzioni interpretative e/o di riforma

Descrizione del lavoro e ruolo dei partecipanti: Tutti i ricercatori contribuiranno all'elaborazione di strumenti rimediali, anche in una prospettiva di riforma, avvalendosi pure del supporto dell'*expertise* ingegneristica. Si prevede una riunione del gruppo di ricerca intermedia, finalizzata all'analisi trasversale dei dati e alla selezione delle proposte risolutive, una riunione conclusiva, finalizzata alla sistemazione dei risultati, l'organizzazione di un'iniziativa seminariale rivolta a dottorandi e studenti, l'organizzazione di un convegno interdisciplinare finale (anche con studiosi di aree scientifiche diverse dall'area 12) avente a oggetto le soluzioni elaborate.

Attività n.3

Obiettivi: Analisi ricognitiva

Descrizione del lavoro e ruolo dei partecipanti: I ricercatori appartenenti al SSD IUS 17, ING-INF/05 e la Direttrice del *Grenoble Alpes Cybersecurity Institute* saranno impegnati, con il coinvolgimento di esperti del settore, membri di funzioni aziendali e esponenti delle associazioni di categorie, nella ricognizione degli assetti procedurali in funzione preventiva del *cybercrime* e a difesa dal medesimo, implementati negli enti collettivi, al fine di individuare potenziali profili di criticità procedurali. Si prevede una riunione del gruppo di ricerca intermedia, finalizzata al confronto sui dati acquisiti, e una conclusiva, funzionale alla sistemazione dei risultati.

Attività n.4

Obiettivi: Proposte migliorative e elaborazione di una procedura “pilota”

Descrizione del lavoro e ruolo dei partecipanti: I ricercatori appartenenti al SSD IUS 17, ING-INF/05 e la Direttrice del *Grenoble Alpes Cybersecurity Institute* contribuiranno all’elaborazione di proposte risolutive dei profili di criticità procedurali e alla costruzione di una procedura “pilota” preventiva del rischio-c*ybercrime*. Si prevede una riunione del gruppo di ricerca intermedia, finalizzata alla soluzione delle proposte rimediali, una riunione conclusiva, finalizzata alla loro definitiva messa a punto, l’organizzazione di un’iniziativa seminariale rivolta a dottorandi e studenti, l’organizzazione di un convegno interdisciplinare finale (anche con studiosi di aree scientifiche diverse dall’area 12) avente a oggetto le soluzioni elaborate, l’organizzazione di un’iniziativa di *public engagement*, tramite incontro con le comunità locali, funzionale alla condivisione in chiave divulgativa dei benefici della ricerca nella prospettiva di educare i singoli alla difesa dai *cybercrimes*.

1.4 Destinazione editoriale dei risultati della ricerca:

Indicare quale tipo di destinazione si intende dare ai risultati della ricerca specificando come si prevede di soddisfare la condizione di pubblicare in riviste di fascia A e/o Scopus o Wos e/o online open access:

Si prevede la pubblicazione di due saggi in riviste scientifiche giuiridiche di fascia A, preferibilmente in *open access*, e di un articolo in rivista scientifica ingegneristica indicizzata Scopus o Wos.
Si prevede la pubblicazione di un volume collettaneo (atti del primo convegno) presso una casa editrice di primaria importanza, che garantisca la diffusione del prodotto quantomeno a livello nazionale.
Il sito web “Laboratorio Diritto e innovazione” garantirà la diffusione del materiale elaborato nel corso dello sviluppo del progetto.

2. Implementazione (massimo 7000 caratteri, spazi bianchi e tabelle escluse)

2.1 Responsabile Scientifico

Fornire un profilo scientifico del Responsabile scientifico con attinenza al progetto.

A.F. Tripodi ha partecipato al progetto di ricerca *“Innovation4Inclusion*” (2020-2022) e partecipa al Programma di Ricerca e Innovazione “*Innovation, digitalisation and sustainability for the diffused economy in Central Italy - VITALITY*” nell’ambito dello Spoke 1 “MEGALITHIC: *MEthods and technoloGies enhAncing Local specIalization sTrategies in Health, Industry and Cybersecurity”*. Membro del collegio dei docenti del Dottorato di ricerca in *Diritto e innovazione* dell’Univ. di Macerata, è stato componente del Comitato scientifico della Commissione di riforma in materia di responsabilità da reato degli enti (Min. Economia e Giustizia, 2016) e di quello della Commissione di riforma in materia di sistema sanzionatorio (Min. Giustizia, 2014). Al tema della responsabilità da reato degli enti ha dedicato la monografia *L’elusione fraudolenta nel sistema della responsabilità da reato degli enti*, 2013. In materia di responsabilità penale e nuove tecnologie ha pubblicato: *Uomo,* societas*,* machina, in *Studi in onore di C. E. Paliero*, 2022; *Abusi di mercato e* trading *algoritmico*, in *Il diritto nell’era digitale*, 2022. È intervenuto come relatore in numerosi

convegni, tra i quali *International Conference on Information Law*, con una relazione dal titolo "*The Fight against Cybercrime in Italy: Between Reactive and Proactive Approaches*", Shen Junru Law School, Hangzhou Normal University (2021).

2.2 Gruppo di ricerca nel suo complesso

Per ogni membro dello staff di ricerca fornire una breve descrizione della precedente esperienza attinente alle attività assegnate.
Descrivere come i partecipanti nel loro complesso costituiscono un gruppo capace di raggiungere gli obiettivi di progetto. Descrivere come essi sono adatti a svolgere le attività loro assegnate e come si impegnano ad implementarle.
Mostrare la complementarietà tra i partecipanti. Spiegare come la composizione del gruppo di ricerca è ben bilanciata in relazione agli obiettivi del progetto. Se appropriato, descrivere il coinvolgimento di imprese per assicurare lo sfruttamento dei risultati e come sia stata data attenzione all'opportunità di coinvolgere le PMI. Evidenziare il tratto della interdisciplinarietà.

E. Calzolaio è stato Direttore del Dip. di Giurisprudenza dell'Univ. di Macerata (2012-2018) ed è Coord. del Dip. di Eccellenza (2023-2027) su "*Innovazione e vulnerabilità: problemi giuridici e tutele*". Ha partecipato a progetti di ricerca di interesse nazionale (PRIN) e europei. I suoi principali interessi di ricerca riguardano il confronto *civil law-common law* rispetto al diritto dei contratti e alle nuove tecnologie (dati, criptovalute, NFT).

C. Cesari è docente, tra l'altro, di *Criminal procedure and new technologies*. Ha partecipato come responsabile o coordinatrice a numerosi progetti di ricerca, fra cui *Uni4Justice* (2022-2023), *Protecting young suspects in interrogations* (2012), *Innovation4Inclusion* (2020-2022), PRIN 2022 *Nuove tecnologie, dati biometrici e procedimenti penali*. I suoi principali interessi di ricerca riguardano i temi della prova penale, dell'impatto sul rito penale delle nuove tecnologie, della tutela dei soggetti vulnerabili in tale rito.

F. Marongiu Buonaiuti ha partecipato al progetto di ricerca *The Europeanization of Private International Law of Successions* (2013) e partecipa a *EJNITA Building Bridges*. Alle questioni di giurisdizione civile degli illeciti *online* ha dedicato gli scritti: *La disciplina della giurisdizione nelle controversie civili relative ad attività on-line: coerenza e varietà di orientamenti nei principali ambiti di rilievo,* in *Nuovo dir. civ.*, 2018; *Jurisdiction Concerning Actions by a Legal Person for Disparaging Statements on the Internet: The Persistence of the Mosaic Approach,* in *European Papers*, 2022. In tema di mercati e servizi digitali ha pubblicato *L'ambito di applicazione territoriale del Digital Markets Act e del Digital Services Act.,* in *Verso una legislazione europea su mercati e servizi digitali*, 2021.

C. Piergallini è stato membro delle Commissioni ministeriali incaricate di elaborare le principali riforme in materia penale della legislatura 1997-2001, della Commissione di riforma in materia di sistema sanzionatorio (Min. Giustizia, 2014) e della Commissione di riforma in materia di responsabilità da reato degli enti (Min. Economia e Giustizia, 2016). Tema, quest'ultimo, a cui ha dedicato numerosi scritti. Ha partecipato a vari progetti di ricerca, tra cui *La riforma del codice penale* (2003). In materia di responsabilità penale e nuove tecnologie ha pubblicato *Intelligenza artificiale: da 'mezzo' a 'autore' del reato?*, in *Riv. it. dir. proc. pen*., 2020.

R. Acquaroli ha partecipato a vari progetti di ricerca, tra cui *Criminal Preventive Risk Assessment in the Law-Making Procedure* (2001). Ha svolto ricerche sul contrasto alla circolazione della ricchezza illecita e *blockchain*, nonché sull'uso delle piattaforme in danno ai soggetti vulnerabili. In materia ha pubblicato: *Blockchain and criminal risk*, in *Legal tecnology trasformation. A Practical Assessment*, 2020; *Cyberbullismo e hate speech. Alcune considerazioni sulla l. n. 71/2017*, in *I linguaggi dell'impresa,* 2021.

L. Bartoli è stata titolare di assegni di ricerca in tema di *digital investigation* e *prova digitale*. Tra i suoi scritti: *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo*, in *Leg. pen.*, 2022; *Digital evidence for the criminal trial: limitless cloud and state boundaries*, in *EuroJus*, 2019; *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen.*, 2018. Ha partecipato ai progetti di ricerca EVIDENCE, DEVICES, CrossJustice, Force, EuDiCRI, EcoCyber. È membro dell'azione COST "*Digital forensics: evidence analysis via intelligent systems and practices (DigForASP)*" – CA17124 ed è consulente dell'Ufficio della Conv. di Budapest in materia di *cybercrime* e crimine informatico.

P. Sernani è leader del WP3 del progetto di ricerca TRUST *digital TuRn in EUrope: Strengthening relational reliance through Technology* e membro del PRIN 2022 PNRR *Normative and Digital Solutions to Counter Threats during National Election Campaigns (RightNets)*. Sui temi legati alla sicurezza e al trattamento dei dati, è coautore, tra le altre, delle pubblicazioni: *FRMDB: Face recognition using multiple points of view*, *Sensors*, vol. 23, no. 4, 2023; *Deep Learning for Automatic Violence Detection: Tests on the AIRTLab Dataset*, *IEEE Access*, vol. 9, 2021; *Violence detection in videos by combining 3D convolutional neural networks and support vector machines, Applied Artificial Intelligence*, vol. 34, 2020. Sugli stessi temi ha relazionato in due ediz. delle conferenze internazionali IEEE MetroXRAINE (2022, 2023) e RTA-CSIT (2021, 2023).

S. Zolea è docente dei corsi *Diritto comparato dei dati* e *dell'Intelligenza Artificiale* e *European and Comparative Data Law*. È autore o coauture di numerose scritti in materia, tra cui *Pubblicità e accesso alle decisioni giudiziarie alla prova delle nuove tecnologie*, in *Pol. dir.*, 2022; *European courts and predictive justice: a feasible symbiosis?*, in *Opinio Juris in Comp.*, 2023. È stato membro (2019-2021) del progetto di *ricerca Decision And New Technology* del Dip. di Eccellenza di Giurisprudenza dell'Univ. di Macerata.

K. Bannelier è direttrice del *Grenoble Alpes Cybersecurity Institute* e co-direttrice della cattedra di *Legal and Regulatory Implications of Artificial Intelligence*. E' autrice di numerose pubblicazioni in materia di sicurezza internazionale con particolare riguardo al cyberspazio.

Il gruppo si compone di studiosi con competenze poliedriche, ossia non limitate al piano scientifico *tout court*, ma estese a quello attuativo-progettuale. L'*expertise* nei vari settori, connotata da tratti specialistici riguardo all'ambito di riferimento, dimostra l'attitudine dei partecipanti a svolgere un'analisi approfondita della materia e a produrre risultati apprezzabili quali esiti scientificamente innovativi. Le varie esperienze in campo progettuale garantiscono l'abilità allo svolgimento di attività di *équipe* e la partecipazione ad esperienze di progettazione normativa di rilievo istituzionale attesta la capacità di elaborazione di proposte di riforma.
La composizione del gruppo riflette il "peso", in termini di contributo agli esiti, riconoscibile alla disciplina di appartenenza: si giustifica così il più elevato numero di esperti nelle materie

della macroarea penalistica, a cui segue quello dei comparatisti del diritto privato e degli internazionalisti, dato il carattere transnazionale e sovranazionale del tema; e infine, l'*expertise* ingegneristica, che si rivela fondamentale in ragione della marcata *technicality* del fenomeno cibernetico.
Il coinvogimento di associazioni di categoria e funzioni aziendali consente un proficuo confronto soprattutto ai fini dell'individuazione di criticità procedurali negli enti collettivi.

3. Impatto (massimo 3000 caratteri, spazi bianchi e tabelle esclusi)

3.1 Impatto previsto rispetto alla implementazione del Dipartimento di eccellenza

Illustrare la rilevanza della ricerca proposta rispetto al progetto del Dipartimento di eccellenza:

La ricerca proposta è immediatamente correlata al progetto del Dipartimento di eccellenza "Innovazione e vulnerabilità: problemi giuridici e tutele*"*, esprimendo una piena corrispondenza con ciascuno dei suoi referenti concettuali: *innovazione*, rappresentando il *cyberspace* uno dei risvolti più significativi del moderno sviluppo tecnologico; *vulnerabilità*, impersonata dalla figura dell'utente della rete, pienamente inquadrabile nell'ambito elettivo delle *nuove vulnerabilità*, data la relativa dimensione universale, ossia non circoscritta alle tradizionali categorie di soggetti deboli, pur ampiamente colpite dal fenomeno (spesso a causa delle loro minori competenze tecnico-culturali); *problemi giuridici*, sui quali si appunta l'analisi in termini di mappatura dei punti di minore resistenza del sistema nella prospettiva della protezione degli interessi individuali e collettivi; *tutele*, verso cui il progetto è polarizzato, con l'intento di elaborare soluzioni esegetiche, direttrici di riforma, modelli procedurali prevenzionistici del *cyber*-rischio.

3.2 Disseminazione e/o sfruttamento dei risultati di progetto

Descrivere le misure proposte per la disseminazione e/o lo sfruttamento dei risultati del progetto e come queste aumenteranno l'impatto del progetto.

La disseminazione dei risultati avverrà mediante:

- l'organizzazione di due convegni interdisciplinari (anche con studiosi di aree scientifiche diverse dall'area 12) attraverso i quali rendere pubblici i risultati della ricerca;
- la pubblicazione di un volume-atti del primo dei due convegni previsti;
- la videoregistrazione del secondo dei due convegni, accessibile sul sito web del "Laboratorio diritto e innovazione";
- due iniziative seminariali destinate a dottorandi e studenti;
- organizzazione di un'iniziativa di *public engagement*, tramite incontro con le comunità locali, funzionale alla condivisione in chiave divulgativa dei benefici della ricerca nella prospettiva di educare i singoli alla difesa dai *cybercrimes*;
- la pubblicazione di due saggi su riviste scientifiche giuridiche di fascia A, preferibilmente in *open access*, e di un articolo su rivista scientifica ingengneristica indicizzata Scopus o Wos;
- il caricamento di materiale (anche sottoforma di *slides*) didattico, di studio, divulgativo e scientifico, come ad esempio la procedura "pilota" preventiva del rischio reato elaborata dal gruppo di ricerca, sul sito web "Laboratorio Diritto e innovazione".

Attraverso le iniziative elencate si intende assicurare il coinvogimento della più ampia platea di destinatari possibili – dai docenti ai dottorandi, agli studenti, fino alla comunità locale – e al contempo garantire, per via degli strumenti più avanzati, un elevato grado di fruibilità dei risultati del progetto.

3.3 Produzione di materiale scientifico e divulgativo per il sito web del "Laboratorio di innovazione"

Illustrare in che modo il progetto potrà contribuire alla offerta di informazioni nel sito web del Laboratorio Diritto e Innovazione del Dipartimento di eccellenza

Nella piattaforma del "Laboratorio Diritto e innovazione" saranno inseriti:

- videoregistrazione del secondo convegno programmato;
- tre serie di *slides* su temi centrali della ricerca a scopo didattico e di studio (da utilizzare nei seminari programmati per dottorandi e studenti), contributi scientifici e di tipo divulgativo;
- la procedura "pilota" preventiva del rischio reato elaborata dal gruppo di ricerca.

Responsabile scientifico

Firmato digitalmente da Andrea Francesco Tripodi
Data: 13.11.2023 10:44:46 CET
Organizzazione: UNIVERSITA' DEGLI STUDI DI MACERATA/00177050432