Università di Genova

Linea Guida generale per la sicurezza e l'integrità della ricerca e per la gestione dei rischi dual use e sicurezza della ricerca

1. Premessa

L'Università degli Studi di Genova riconosce la libertà della ricerca scientifica, della didattica, della collaborazione internazionale e della circolazione della conoscenza come elementi essenziali della propria missione pubblica. La ricerca universitaria si fonda su apertura, confronto, cooperazione, integrità, responsabilità e autonomia scientifica.

Nel contesto internazionale attuale, tuttavia, la ricerca può essere esposta a rischi nuovi o accresciuti: sottrazione di dati e risultati, uso improprio di conoscenze, trasferimento indesiderato di tecnologie critiche, interferenze indebite, vulnerabilità cyber, perdita di controllo su asset scientifici, violazione di obblighi normativi, rischi connessi a collaborazioni e finanziamenti esterni, nonché possibili impieghi dual use di beni, software, tecnologie, dati e know-how.

Le collaborazioni accademiche internazionali, sempre più frequenti e complesse, impongono inoltre di strutturare i progetti in modo compatibile non solo con il quadro europeo, ma anche con eventuali partnership con enti e istituzioni di Paesi terzi, inclusi Stati Uniti, Regno Unito e altri Paesi extra-UE. In tali contesti, la presenza di policy chiare in materia di sicurezza della ricerca, dual use, export control, accesso ai dati, open science e trasferimento di conoscenza costituisce un requisito di affidabilità, continuità e qualità della collaborazione scientifica.

La presente Linea Guida, che si appoggia al manuale operativo interno ed alle schede progetto, intende fornire un quadro generale di Ateneo per integrare due dimensioni strettamente collegate:

1. **sicurezza e integrità della ricerca**, intesa come protezione dei metodi, dei dati, dei risultati, delle collaborazioni e dell'ambiente accademico da furto, uso improprio, sfruttamento indebito, interferenze e violazioni dei valori fondamentali della ricerca;

2. **compliance dual use / export control**, intesa come gestione degli obblighi relativi al monitoraggio sulla esportazione di beni, software, tecnologie, dati e know-how a duplice uso, inclusi trasferimenti fisici e intangibili.

La Linea Guida non introduce un modello di chiusura o un ulteriore, indesiderabile, adempimento burocratico. Al contrario, mira a preservare una ricerca aperta, internazionale e responsabile, rafforzando la capacità dell'Ateneo di riconoscere e mitigare rischi specifici prima che producano conseguenze normative, reputazionali, scientifiche o di sicurezza a danno dei singoli ricercatori e della Istituzione.

2. Finalità

La presente Linea Guida ha le seguenti finalità:

- promuovere una cultura condivisa della sicurezza e integrità della ricerca;
- favorire la cooperazione internazionale aperta, sicura e responsabile;
- tutelare la libertà accademica, evitando limitazioni non necessarie;
- supportare ricercatori, docenti, collaboratori, dipartimenti e strutture amministrative nelle loro attività di collaborazione internazionale a riconoscere situazioni a rischio ed evitare possibili implicazioni legali;
- rafforzare la capacità dell'Ateneo di prevenire sottrazione, uso improprio o trasferimento indesiderato di dati, risultati, tecnologie e competenze;
- assicurare una gestione proporzionata degli obblighi inerenti al dual use / export control;
- integrare i dettami della sicurezza della ricerca, dual use ed export control con open science, cybersecurity, protezione dei dati, trasferimento tecnologico e collaborazioni internazionali;
- garantire tracciabilità, proporzionalità e coerenza nelle decisioni;
- ridurre il rischio di violazioni normative, danni reputazionali, perdita di asset scientifici, uso improprio dei risultati e compromissione dei diritti fondamentali;
- rafforzare l'affidabilità dell'Ateneo come partner di progetto in reti europee, transatlantiche e internazionali.

3. Ambito di applicazione

La presente Linea Guida si applica alle attività di ricerca, didattica avanzata (III livello), innovazione, trasferimento tecnologico, knowledge transfer, collaborazione scientifica e gestione infrastrutturale dell'Ateneo che possano comportare profili di rischio per la sicurezza e integrità della ricerca o per la compliance dual use / export control. Lo scopo della Linea Guida è pertanto di suggerire come sia la sicurezza della ricerca e l'export control debbano essere considerati parte del DVR – Documento Valutazione Rischi di Ateneo, e pertanto integrati nei processi già esistenti: proposal, grant, contratti, accordi internazionali, open data, pubblicazioni, accessi IT, accessi a laboratorio, missioni, visiting, spedizioni, procurement, brevetti, licensing, spin-off e attività conto terzi.

4. Documenti di riferimento

La presente Linea Guida è redatta tenendo conto dei seguenti documenti reperibili anche sul sito del Centro Sicurezza, Rischio e Vulnerabilità di UniGe:

- Regolamento (UE) 821/2021 relativo al regime dell'Unione per il controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso;
- Raccomandazione (UE) 1700/2021 della Commissione, relativa ai programmi interni di conformità per i controlli della ricerca che coinvolge prodotti a duplice uso;
- aggiornamenti degli allegati tecnici del Regolamento (UE) 821/2021;
- Raccomandazione del Consiglio dell'Unione europea del 23 maggio 2024 relativa al rafforzamento della sicurezza della ricerca;

- Modello Nazionale per l'Integrità e la Sicurezza della Ricerca del Ministero dell'Università e della Ricerca;
- Linee Guida MUR per le Istituzioni di ricerca;
- Carta dei diritti fondamentali dell'Unione europea, con particolare riferimento alla libertà della ricerca scientifica e ai principi di legalità, necessità e proporzionalità;
- Statuto dell'Università degli Studi di Genova;
- Codice etico dell'Università degli Studi di Genova;
- Codice di comportamento dei dipendenti dell'Università degli Studi di Genova;
- disposizioni nazionali applicabili in materia di export control, sicurezza, cybersecurity, protezione dei dati, proprietà intellettuale, anticorruzione, conflitto di interessi e integrità della ricerca;
- fonti istituzionali europee in materia di misure restrittive e sanzioni, inclusa la EU Sanctions Map.

5. Principi generali

5.1 Libertà accademica e responsabilità accademica

La libertà della ricerca scientifica è il presupposto della presente Linea Guida. L'Ateneo tutela la libertà di indagine, pubblicazione, insegnamento e collaborazione scientifica.
Tale libertà si accompagna alla responsabilità accademica: la comunità universitaria è chiamata a prevenire, come da indicazioni nel Regolamento UE 821/2021 e nei limiti ragionevoli delle proprie funzioni, l'uso improprio di conoscenze, tecnologie, dati, strumenti e risultati generati nell'ambito dell'Ateneo. Questo principio si applica sul riconoscimento che solo il ricercatore, nella sua libertà accademica, è conscio di tutti gli aspetti della propria ricerca e di eventuali rischi di malversazione operabile da terzi con le opportune conoscenze.

5.2 Apertura sicura

La cooperazione scientifica internazionale e l'open science sono valori essenziali. L'obiettivo non è ridurre l'apertura, ma renderla più sicura. L'Ateneo adotta il principio: "*as open as possible, as closed as necessary*", comunemente applicato negli ultimi anni in ambito accademico nella Unione Europea. Ciò significa che i risultati della ricerca devono essere condivisi nella misura massima possibile, ma alcune informazioni, dati, software, modelli o tecnologie possono richiedere accesso controllato, redazione, embargo, clausole contrattuali o altre misure proporzionate.

5.3 Proporzionalità

Le misure di sicurezza e compliance devono essere proporzionate al rischio. Non tutte le attività di ricerca così come le collaborazioni internazionali sono a rischio ma per tutte vale il principio di valutarne preventivamente l'esposizione. Tuttavia, quando emergono segnalazioni di possibili rischi, l'Ateneo deve poter attivare controlli mirati e, in conformità al Regolamento UE 821/2021, monitorare quanto esce dai propri laboratori per poter supportare i docenti laddove si trovino in una condizione di esportazione tangibile o intangibile extra UE. La misura preferibile è sempre quella meno restrittiva idonea a mitigare il rischio.

5.4 Legalità e tracciabilità

Le decisioni rilevanti devono essere fondate su norme (Vedi Regolamento UE), linee guida (Vedi Linee Guida MUR), valutazioni tecniche o elementi documentabili. Le indicazioni provenienti dall'Ufficio DU/RS di Ateneo che comportino eventuali limitazioni, prescrizioni, sospensioni, controlli di accesso, richieste di autorizzazione o escalation saranno tracciate in modo da poter garantire sia ai docenti che

all'amministrazione la tempistica e l'efficacia dei provvedimenti assunti per mitigare per quanto possibile il rischio segnalato.

5.5 Approccio risk-based

La Linea Guida adotta un approccio basato sulla analisi del rischio che viene affrontata con maggior dettaglio nel Manuale Operativo DU/RS di Unige. Attualmente sul mondo della ricerca insistono principalmente due tipologie di rischio:

- **Rischio Dual Use**

In questa fattispecie la natura del rischio è basata sulla combinazione di tre elementi: *Il prodotto, l'uso finale, l'utilizzatore finale*. Tutti e tre concorrono a definire, secondo i dettami del Regolamento UE 821/2021, l'eventuale carattere dual use. Queste tre caratteristiche verranno dettagliatamente illustrate nel Manuale Operativo. In questa sede si puo' tuttavia ricordare che:

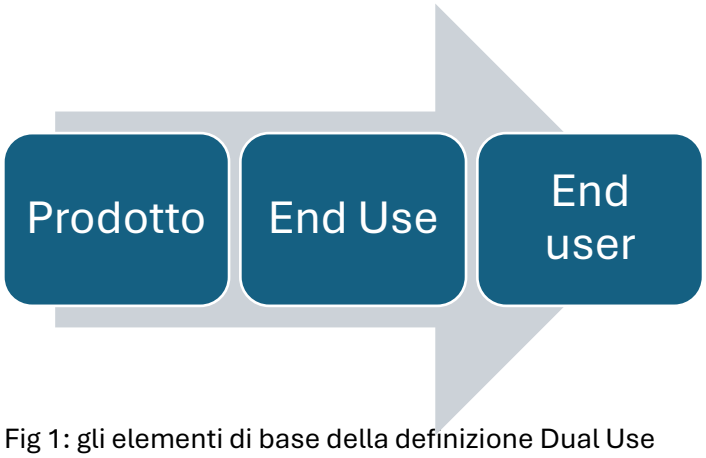

Fig 1: gli elementi di base della definizione Dual Use

- **PRODOTTO**: è quanto si ritrova sull'Annex I o Annex IV del Regolamento UE 821/2021
- **END USE**: è l'uso previsto nelle finalità di progetto
- **END USER**: è il committente o il partner che fruirà di questa innovazione

Risulta gia' chiaro da questo primo spunto la difficoltà di applicazione di questo regolamento nella realtà' accademica:

- Il PRODOTTO, a livello universitario, è spesso non ben identificabile in quanto l'output di ricerca è mediamente a scala TRL medio-bassa.
- L'END-USE potrebbe non essere del tutto chiaro in applicazioni in ambito fisico/chimico/biologico ma anche in certe applicazioni embrionali di Ingegneria.
- L'END USER potrebbe nuovamente essere difficile da identificare laddove per esempio si stia valutando come forma di esportazione una pubblicazione scientifica o altra forma intangibile.

Ne deriva che per poter inquadrare l'eventuale rischio dual use di una innovazione o di un progetto occorrono alcuni dati, sia relativi al progetto in sé, sia alla sua diffusione, al suo finanziamento (sollevando il problema relativo a fondi pubblici sotto open science piuttosto che privati sotto richieste di NDA) così come ai partner coinvolti ed alle persone che lavoreranno nei vari laboratori.

L'attenzione, pertanto, si concentrerà principalmente su:

- natura scientifica o tecnologica dell'attività;
- dati, software, tecnologie e asset coinvolti;
- partner e destinatari;
- fonti di finanziamento;
- Paesi e contesti geopolitici;
- usi finali prevedibili;
- cybersecurity e protezione degli accessi;
- open data e repository;
- mobilità internazionale;
- export control e trasferimenti intangibili.

- **Rischio Research Security**

Come declinato nelle Linee Guida e Modello Nazionale del MUR il rischio in questo caso è costituito essenzialmente da quanto viene descritto come insieme di "*minacce ibride*", ovverossia le circostanze che conducono al consapevole trafugamento dei dati per applicazioni di particolare interesse sia economico che strategico per altre nazioni e/o gruppi industriali.
La mitigazione del rischio in questo caso non riguarda tanto e solamente il Paese di origine dei collaboratori (post-doc, fellowship etc) ma più spesso le procedure generali messe in atto dall'istituto per ridurre la sua esposizione in forma generale, attraverso politiche di informazione e formazione dei docenti, ammodernamento delle infrastrutture critiche etc.

6. Doveri e responsabilità condivise delle componenti di Ateneo

La gestione dei rischi connessi alla sicurezza della ricerca e alla compliance dual use/export control è concepita dall'Ateneo seguendo le indicazioni della Commissione Europea come attività di tutela della comunità scientifica, prima ancora che come adempimento amministrativo.

Il Regolamento UE 2021/821 evidenzia, nelle proprie premesse, che il principio di due diligence, come parte di un Internal Compliance Program (la cui struttura è suggerita nel Manuale UE1700/2021) è particolarmente rilevante per gli organismi di ricerca, nei quali il trasferimento può riguardare non solo beni fisici, ma anche software, tecnologia, dati, modelli, know-how, accessi remoti e attività di assistenza tecnica.

La Raccomandazione UE 1700/2021 chiarisce inoltre che gli organismi di ricerca e i ricercatori sono soggetti agli obblighi previsti dalla disciplina dual use/export control e che un sistema interno proporzionato è essenziale per prevenire rischi di non conformità. La finalità della presente Linea Guida, abbinata al Manuale Operativo, che affiancherà questo documento è quindi anche quella di presentare ai docenti e ai ricercatori un quadro di supporto che consenta di riconoscere tempestivamente le situazioni sensibili, chiedere assistenza, documentare le decisioni e svolgere la ricerca in condizioni di maggiore sicurezza giuridica e istituzionale.

Procedure analoghe di attenzione preventiva alla ricerca a potenziale duplice uso sono ormai comuni e necessarie nei Paesi europei. Esse sono inoltre presenti da tempo nel sistema universitario e di ricerca statunitense, in particolare attraverso le procedure di revisione istituzionale del Dual Use Research of Concern (DURC), sviluppate per identificare, valutare e mitigare i rischi derivanti da ricerche che potrebbero generare conoscenze, prodotti o tecnologie suscettibili di uso improprio. Pur non coincidendo integralmente con il regime europeo di export control, tali esperienze confermano la centralità di un presidio istituzionale preventivo e della collaborazione tra Principal Investigator, strutture di compliance e leadership dell'ente.

L'adozione e l'esposizione trasparente di procedure di sicurezza della ricerca e dual use costituiscono inoltre un elemento di garanzia e qualità nei confronti dei partner di progetto, sia europei sia extra-europei. Un Ateneo dotato di procedure chiare, proporzionate e documentate è un partner più affidabile, perché dimostra di saper proteggere dati, risultati, tecnologie, accessi, proprietà intellettuale, libertà accademica e continuità delle attività scientifiche. La sicurezza della ricerca non è quindi un ostacolo alla cooperazione internazionale, ma una condizione per mantenerla aperta, credibile e sostenibile nel tempo.

Training operativo, manutenzione, configurazione, collaudo, consulenza tecnica, supporto a distanza e trasferimento di know-how possono costituire assistenza tecnica rilevante. Quando riguardano tecnologie sensibili o destinatari a rischio, devono essere valutati prima dell'erogazione.

6.1 Doveri della governance e delle strutture di Ateneo (Sez. 1 – UE 1700/2021)

L'Ateneo, attraverso i propri organi, uffici e strutture competenti, mette a disposizione della comunità universitaria informazioni, risorse, procedure e punti di contatto per assistere docenti, ricercatrici, ricercatori e personale coinvolto nella valutazione dei nuovi progetti e delle attività potenzialmente rilevanti. Le risorse saranno concentrate in un ufficio dedicato alla RS/DU di sicuro riferimento sia per docenti/ricercatori sia per gli organismi esterni (CRUI, Ministeri etc.) con i quali è necessario interagire

In particolare, l'Ateneo, secondo quanto suggerito nel Regolamento UE 821/2021 e nella Sez. 1 del Manuale UE 1700/2021, si impegna a:

- promuovere una cultura della ricerca aperta, sicura, integra e responsabile;
- rendere disponibili informazioni di base sulla normativa dual use / export control e sulla sicurezza della ricerca;
- individuare referenti o strutture di supporto per la gestione dei dubbi e delle segnalazioni;
- predisporre strumenti di autovalutazione preliminare per progetti, collaborazioni, accessi, pubblicazioni, dati, software, spedizioni e attività di trasferimento tecnologico;
- supportare i responsabili scientifici nella lettura dei principali indicatori di rischio;
- integrare la valutazione del rischio nei processi ordinari di Ateneo, quali proposal, grant, contratti, accordi internazionali, data management plan, open data, repository, visiting, accessi IT, missioni, spedizioni e attività conto terzi;
- favorire il coordinamento tra uffici ricerca, ufficio legale, ufficio trasferimento tecnologico, internazionalizzazione, IT security, biblioteche, procurement, strutture dipartimentali e responsabili di laboratorio;
- garantire che eventuali misure limitative siano motivate, proporzionate, tracciabili e rispettose della libertà accademica;
- predisporre attività di formazione e sensibilizzazione differenziate per ruoli e aree di rischio;
- curare l'aggiornamento periodico degli strumenti interni in relazione all'evoluzione normativa europea, nazionale e ministeriale.

La funzione dell'Ateneo non è sostituirsi alla valutazione scientifica del ricercatore, ma fornire un quadro organizzativo che renda possibile una gestione consapevole e tempestiva dei rischi. Il sistema di supporto deve essere accessibile, proporzionato e orientato alla soluzione, evitando appesantimenti non necessari per le attività ordinarie e a basso rischio.

6.2 Doveri di collaborazione dei docenti, ricercatrici e ricercatori (Sez. 2- UE 1700/2021)

La collaborazione della comunità scientifica è essenziale per l'efficacia del sistema. Come evidenziato dalla Raccomandazione UE 1700/2021, i ricercatori e le strutture di ricerca sono nella posizione migliore per conoscere la natura tecnica dei prodotti, delle tecnologie, dei software, dei dati e dei risultati sviluppati nell'ambito delle proprie attività. Docenti, ricercatrici, ricercatori e responsabili scientifici sono pertanto chiamati a collaborare attivamente con le strutture di Ateneo, segnalando tempestivamente eventuali elementi di attenzione. In particolare, essi devono prestare attenzione quando una ricerca, un progetto, una collaborazione o un output scientifico presenti affinità, anche potenziale, con:

- beni, software o tecnologie già elencati nell'Allegato I del Regolamento UE 821/2021 e nei relativi aggiornamenti;
- tecnologie, software, dati, modelli, strumenti, componenti o know-how che, pur non chiaramente listati, possano risultare funzionalmente vicini a prodotti o tecnologie controllate;
- attività che prevedono trasferimenti fisici o intangibili verso Paesi terzi, inclusi cloud, repository, e-mail, piattaforme collaborative, accessi remoti, conferenze online, condivisione di link o comunicazioni tecniche;
- collaborazioni con partner, finanziatori, sub-partner o destinatari per i quali non siano pienamente chiari finalità, uso finale o utilizzatore finale;
- applicazioni potenzialmente pericolose, militari non supportate dalle specifiche piattaforme di controllo, proliferazione, sorveglianza, cyber-offensive, intelligence, repressione o comunque idonee a generare effetti nocivi per la sicurezza pubblica, la sicurezza internazionale, i diritti umani o il diritto internazionale umanitario;
- richieste anomale di accesso a dati, software, infrastrutture, laboratori, campioni, prototipi, parametri, procedure operative o risultati non pubblicati;
- condizioni contrattuali o collaborative che limitino in modo non ordinario la pubblicazione, impongano riservatezza non giustificata, prevedano ri-trasferimenti non chiari o attribuiscano diritti di uso ampi e non proporzionati rispetto allo scopo scientifico.
- Materiale speciale contenuto nell'Annex IV del Regolamento UE 821/2021

La segnalazione di un dubbio non implica il blocco dell'attività. Essa consente invece di svolgere una verifica proporzionata, individuare eventuali misure di mitigazione e tutelare sia il ricercatore sia l'Ateneo.

La responsabilità del ricercatore consiste, in particolare, nel:

- descrivere in modo accurato la natura tecnica dell'attività e degli output attesi;
- compilare le schede di autovalutazione del progetto;
- segnalare tempestivamente red flags tecniche, collaborative o di destinazione;
- non procedere autonomamente, nei casi dubbi, a trasferimenti, pubblicazioni, condivisioni o spedizioni potenzialmente rilevanti;
- rispettare le misure concordate con le strutture competenti, quali redazione, accesso controllato, limitazione degli accessi, embargo, clausole contrattuali o verifiche prima della spedizione;
- contribuire alla conservazione delle evidenze e alla tracciabilità delle decisioni.

6.3 Ruolo del Manuale operativo di compliance (Sez. 3 – UE 1700/2021)

Il processo applicativo focalizzato ad implementare le indicazioni normative sarà strutturato in un separato Manuale operativo di compliance per la sicurezza della ricerca e il dual use / export control, predisposto in coerenza con la sezione 3 della Raccomandazione UE 1700/2021. Il Manuale operativo avrà natura pratica e procedurale. Esso dovrà descrivere in modo dettagliato:

- il flusso di screening dei nuovi progetti e delle nuove collaborazioni;
- le checklist di autovalutazione per ricercatori e strutture;
- i criteri di individuazione delle attività affini a prodotti, software o tecnologie dell'Allegato I del Regolamento UE 821/2021;
- le modalità di valutazione di end-use ed end-user;
- le red flags relative a sicurezza della ricerca, diritti umani, uso militare, proliferazione, sorveglianza e cyber risk;
- i processi di escalation verso i referenti competenti;
- le modalità di gestione dei repository, dell'open data, dei software, dei modelli e dei materiali supplementari;
- le procedure per visiting, mobilità, accessi a laboratori, accessi IT, HPC e cloud;
- le procedure per spedizioni, trasferimenti fisici, hand-carry e assistenza tecnica;
- i modelli di registro decisionale e recordkeeping;
- le misure di mitigazione standard;
- i casi pratici e gli esempi applicativi;
- i flussi di comunicazione interna e formazione.

Il Manuale operativo sarà predisposto separatamente, aggiornato periodicamente e utilizzato come strumento di supporto quotidiano per rendere applicabili i principi della presente Linea Guida.

6.4 Finanziamenti Pubblici e Open Data

In conformità con gli obblighi relativi a finanziamenti pubblici in campo europeo l'Ateneo promuove l'open science e l'open data, ma riconosce che l'apertura deve essere compatibile con sicurezza, integrità, protezione dei dati, proprietà intellettuale ed export control.

6.5 Finanziamenti privati

Laddove i progetti possano godere di finanziamenti di tipo privato (per esempio nei casi della fattispecie di "assistenza tecnica") dal punto di vista dual use non si puo' più arrogare la nicchia di esenzione dai controlli per "ricerca di base" (Vedi Manuale UE 1700/2021). Diventa quindi importante avere, per quanto possibile, una chiara visione della provenienza e dei limiti imposti dal finanziatore al libero sviluppo tecnologico e scientifico del progetto, anche rispetto a eventuali condizioni, vincoli, diritti di accesso, obblighi di riservatezza, indirizzamento della ricerca, diritti sui risultati e possibilità di trasferimenti indesiderati. Inoltre, eventuali opacità introdotte dai vincoli contrattuali potrebbero non essere allineate con le necessità inerenti alla sicurezza della ricerca come declinato presso il MUR.

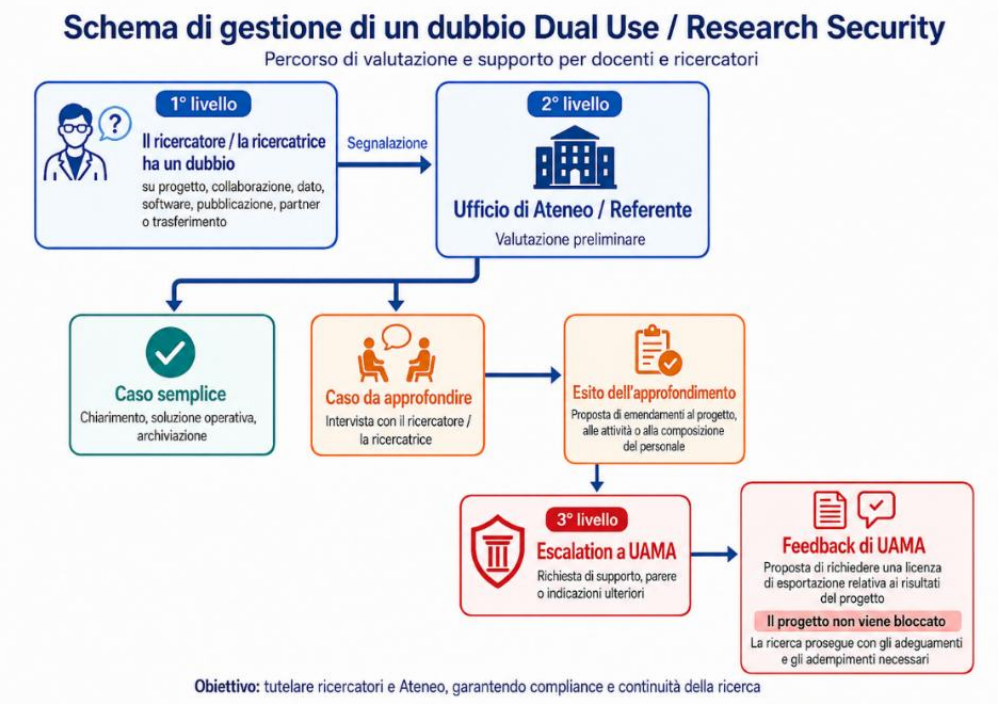

Figura 2 – Schema di gestione di un dubbio Dual Use / Research Security

7. Governance di Ateneo

7.1 Organi di Ateneo

Gli Organi di Ateneo promuovono una cultura della ricerca aperta, sicura e responsabile. Essi approvano indirizzi generali, promuovono il coordinamento tra strutture e assicurano che la sicurezza della ricerca sia integrata nei processi istituzionali.

7.2 Referente per la sicurezza della ricerca

In conformità al Regolamento UE 821/2021 ed alle indicazioni del Manuale UE 1700/2021 l'Ateneo individua una commissione apposita presieduta da un referente ed un Ufficio Amministrativo per la funzione relativa alla sicurezza della ricerca ed alla tematica dei beni e tecnologie dual use/export control. Tale funzione opera come punto di raccordo tra governance, dipartimenti, strutture amministrative e organismi nazionali ed internazionali competenti, comprese le associazioni accademiche operative all'estero su queste tematiche.

La commissione presieduta dal referente supporta l'Ateneo in materia di:

- formazione e comunicazione interna;
- autovalutazione preliminare delle attività;
- analisi delle collaborazioni e dei finanziamenti esterni;
- definizione di misure di mitigazione;
- raccordo con IT security, uffici ricerca, legale, TTO, internazionalizzazione e procurement;
- raccolta e aggiornamento delle informazioni sulle collaborazioni esterne;

- gestione delle escalation;
- screening di beni, software, tecnologie, dati e know-how;
- valutazione dei trasferimenti fisici e intangibili;
- identificazione di possibili obblighi autorizzativi;
- gestione di spedizioni e trasferimenti;
- supporto a open data, repository e pubblicazioni sensibili;
- formazione sui controlli export;
- interlocuzione con autorità competenti, ove necessario.

L'Area Ricerca, Trasferimento Tecnologico e Terza Missione presidierà la casella di posta, a cui si dovranno inviare le schede: **sicurezzaricerca_dualuse@unige.it.** Fornirà, inoltre, il supporto gestionale alla commissione presieduta dal referente, organizzerà la raccolta delle schede progetto, la loro archiviazione e mantenimento dei dati secondo i termini prescritti dalla normativa. Verrà anche conservato tutto lo scambio di informazioni con i referenti dipartimentali e le autorità nazionali, in accordo con la Commissione.

7.3 Coordinamento integrato

La sicurezza della ricerca e l'export control richiedono un coordinamento stabile di:

- dipartimenti e centri;
- aree dirigenziali competenti in materia;
- responsabili di laboratorio;
- responsabili scientifici dei progetti.

Il coordinamento sarà funzionalmente svolto da una commissione, denominata "Cabina di Regia per la sicurezza e l'integrità della ricerca e per la gestione dei rischi dual use e sicurezza della ricerca" formata da docenti ed amministrativi delegati dal MR/DG dell'Ateneo con incarico triennale.

Questa si riunirà periodicamente, su convocazione del referente. Lo stesso potrà indire sedute straordinarie in caso di necessità urgenti e improrogabili. La modalità potrà essere sia in presenza, che in via telematica.

La commissione presieduta dal referente di Ateneo, con il supporto dell'area Ricerca, Trasferimento tecnologico e Terza Missione, presenterà annualmente la valutazione globale della esposizione di Ateneo ai rischi sopra menzionati basata sulle informazioni centrali e quelle fornite dai Dipartimenti in relazione ai progetti, alle collaborazioni in essere ed agli accordi in corso. Una volta deliberata, la relazione verrà presentata in Senato Accademico e in Consiglio di Amministrazione.

7.4 Responsabili scientifici

I responsabili di progetto, attività, laboratorio, collaborazione o programma didattico avanzato sono i primi soggetti in grado di riconoscere criticità tecniche e scientifiche. Essi sono tenuti a collaborare con le strutture competenti, compilare le schede di autovalutazione ove richieste e segnalare tempestivamente dubbi o red flags.

7.5 Conflitti di interesse e conflitti di impegno

La sicurezza della ricerca include la gestione di conflitti di interesse e conflitti di impegno. I ricercatori devono dichiarare, secondo le regole di Ateneo, situazioni che possano influenzare l'indipendenza della ricerca, la gestione dei dati, la pubblicazione dei risultati o l'accesso di soggetti esterni.

Fig. 3: Draft schema di lavoro di UniGe

8. Mobilità, viaggi e visitatori

8.1 Missioni all'estero

Per missioni, conferenze, visite a laboratori esteri o attività presso partner esterni, occorre valutare, come suggerito nelle Linee Guida del MUR:

- destinazione e transito;
- materiali trasportati;
- laptop e supporti digitali;
- software e dati presenti sui dispositivi;
- presentazioni tecniche;
- prototipi o campioni;

- incontri programmati;
- eventuali richieste di accesso a sistemi o repository durante la missione.

Il trasporto personale di laptop, hard disk, USB, campioni, componenti o prototipi può avere rilievo. Nei casi sensibili, il personale deve valutare preventivamente cosa portare e quali dati o software mantenere sui dispositivi.

8.2 Visitatori e delegazioni

Le visite di personale esterno, delegazioni, consulenti o visiting devono essere gestite tramite un protocollo proporzionato. Per visite ordinarie può essere sufficiente una gestione amministrativa standard. Per visite in laboratori o progetti sensibili occorrono controlli più specifici concordati in funzione del rischio configurato.

9. Cybersecurity e protezione dei dati

La sicurezza informatica è parte integrante della sicurezza della ricerca. Le misure cyber devono essere proporzionate alla criticità degli asset.

9.1 Incidenti cyber con impatto sulla ricerca

Un incidente cyber può diventare anche incidente di sicurezza della ricerca quando coinvolge dati, risultati, tecnologie, accessi, proprietà intellettuale o collaborazioni sensibili. In tali casi, IT security e referente sicurezza ricerca devono coordinarsi.

In coerenza con le disposizioni della Direttiva UE 2022/2555 (NIS2) e con l'articolo 24, comma 2, lettera f), del Decreto Legislativo 4 settembre 2024, n. 138, i soggetti rientranti nel perimetro delle presenti linee guida adottano adeguate misure di protezione crittografica, commisurate alla natura delle informazioni trattate e ai rischi connessi.

A tal fine, essi assicurano l'utilizzo di canali di comunicazione cifrati e, ove appropriato, la protezione crittografica dei dispositivi, dei supporti di memorizzazione e degli archivi digitali impiegati per la conservazione, l'elaborazione o il trasferimento delle informazioni rilevanti ai fini della normativa sui beni e le tecnologie a duplice uso.

10. Clausola di bilanciamento

La presente Linea Guida è applicata nel rispetto della libertà della ricerca scientifica, della libertà accademica, dell’autonomia universitaria e dei principi di proporzionalità, legalità e necessità.

Eventuali misure limitative, quali differimento di pubblicazione, controlled access, embargo, limitazione di accessi, sospensione di trasferimenti o richiesta di autorizzazione, sono adottate solo quando giustificate da un rischio concreto o da un obbligo normativo, e devono essere motivate e documentate.

L’obiettivo dell’Ateneo è preservare una ricerca aperta, sicura, responsabile e internazionalmente collaborativa

Glossario (selezione della terminologia riportata nel Regolamento UE 821/2021 e UE 1700/2021)

- Sicurezza della ricerca

Protezione di metodi, dati, risultati, infrastrutture, collaborazioni e asset scientifici da furto, uso improprio, sfruttamento inappropriato, interferenze, trasferimenti indesiderati e altre condotte che possano compromettere integrità, libertà e valore della ricerca.

- Integrità della ricerca

Aderenza a valori, principi e pratiche che mantengono la ricerca onesta, responsabile, affidabile e socialmente utile.

- Dual Use

Beni, software o tecnologie che possono avere uso civile e militare o comunque rientrare nei controlli previsti dalla normativa export control. (Regolamento UE 821/2021 e seguenti)

- Export Control

Insieme di regole che disciplinano esportazione, trasferimento, intermediazione, transito e assistenza tecnica relativi a beni, software e tecnologie controllati.

- Trasferimento intangibile

Trasmissione non fisica di dati, software, tecnologia o know-how tramite e-mail, cloud, repository, accesso remoto, videochiamata, download, link o comunicazione orale.

- Technology Transfer

Trasferimento strutturato di tecnologie, risultati applicativi, prototipi, software, brevetti, componenti, procedure, dati tecnici o know-how industrializzabile verso soggetti esterni all'Ateneo, normalmente a TRL medio-alto.

- Knowledge Transfer

Circolazione, anche informale, di conoscenze scientifiche, competenze tecniche, metodi, capacità operative, dati, interpretazioni, procedure, training o know-how, anche a basso TRL e nell'ambito della ricerca di base.

- Tecnologia

Informazioni specifiche necessarie per sviluppo, produzione o uso di un bene o processo. Può includere disegni, schemi, parametri, formule, protocolli, manuali, istruzioni, modelli o know-how.

- Software

Programmi, codice sorgente, codice oggetto, firmware, script, toolchain o altri componenti digitali.

- Assistenza tecnica

Supporto tecnico, formazione, consulenza, configurazione, manutenzione, collaudo o trasferimento operativo di competenze.

- End-user

Utilizzatore finale di un bene, software, dato, tecnologia o know-how.

- End-use

Uso finale previsto o ragionevolmente prevedibile di un bene, software, dato, tecnologia o know-how.

- Collaborazione esterna

Collaborazione con soggetti esterni all'Ateneo, in particolare con soggetti extra-UE, soggetti privati, partner non pubblici o entità che possono incidere su accessi, risultati, finanziamenti o uso dei dati.

- Finanziamento esterno

Finanziamento proveniente da soggetti pubblici o privati esterni all'Ateneo, con particolare attenzione a finanziamenti extra-UE o privati.

- Due diligence

Verifica proporzionata di partner, finanziatori, destinatari, uso finale, contesto, assetti e condizioni della collaborazione.

- Red flag

Indicatore di possibili criticità, come richieste anomale, mancanza di trasparenza, accessi non proporzionati, vincoli insoliti, partner non chiari o uso finale ambiguo.

- Open science

Approccio alla ricerca basato su apertura, accessibilità e condivisione dei risultati, compatibilmente con sicurezza, integrità, privacy, proprietà intellettuale e obblighi normativi.

- Controlled access

Modalità di accesso regolata da richiesta, autorizzazione, condizioni d'uso e tracciamento.

- Embargo

Differimento temporaneo della pubblicazione o dell'accesso a dati, software, risultati o materiali.

- Deemed export

Concetto proprio del sistema statunitense secondo cui il rilascio di tecnologia controllata a una persona straniera all'interno del territorio nazionale può essere trattato come esportazione verso il Paese di appartenenza della persona. Nel sistema europeo non opera in modo identico, ma esistono situazioni funzionalmente simili che richiedono attenzione, soprattutto in presenza di visiting, accessi a tecnologia controllata, assistenza tecnica e trasferimento successivo verso Paesi terzi.

- Sanzioni ed embargo

Misure restrittive adottate dall'Unione europea nei confronti di Paesi, soggetti, entità, settori, beni, servizi o attività. Possono incidere su collaborazioni, finanziamenti, assistenza tecnica, trasferimenti, formazione, accessi a tecnologie e rapporti con determinati partner.

- ICP – Internal Compliance Program

Programma interno di conformità composto da policy, ruoli, procedure, formazione, controlli, registrazioni e misure tecniche per gestire rischi Dual Use ed export control.

Disposizioni finali

La presente Linea Guida costituisce una base generale di Ateneo. Essa potrà essere integrata da procedure operative, schede di autovalutazione, checklist dual use, protocolli per visitatori, linee guida per viaggi, clausole contrattuali, istruzioni per repository, modelli DMP, registri decisionali e percorsi formativi.

La Linea Guida è soggetta ad aggiornamento periodico in relazione all'evoluzione normativa, agli aggiornamenti europei e nazionali, alle indicazioni del MUR, alle esperienze applicative dell'Ateneo e ai casi concreti emersi.

L'obiettivo è costruire un sistema UniGe di ricerca aperta, sicura, integra e responsabile, capace di proteggere libertà accademica, collaborazione internazionale, dati, risultati, tecnologie e reputazione istituzionale.