Sintesi

Sono numerosi i fattori che rendono la lotta contro la cibercriminalità un compito complesso e unico nel suo genere. Per sua natura, la cibercriminalità non conosce confini e si evolve rapidamente, talvolta più velocemente della capacità di contrasto delle autorità nazionali. La complessità del fenomeno è ulteriormente accresciuta dal suo carattere orizzontale: al giorno d'oggi quasi ogni tipologia di reato può esplicarsi tramite Internet. A causa della volatilità dei dati la raccolta delle prove elettroniche di tali reati può essere difficile e richiedere competenze specifiche. La cooperazione giudiziaria è essenziale per assicurare tempestivamente le prove elettroniche, garantendone l'ammissibilità nei procedimenti giudiziari. La cooperazione giudiziaria internazionale può essere ostacolata dalle profonde differenze esistenti tra i sistemi giuridici nazionali (ad esempio per quanto riguarda la rilevanza penale dei comportamenti o la normativa sulla conservazione dei dati) e dai conflitti di giurisdizione. L'intero fenomeno della cibercriminalità sta modificando il concetto giuridico tradizionale del principio di territorialità, per effetto della natura sovranazionale delle prove necessarie per perseguire efficacemente i criminali informatici.

Pertanto, un'efficace risposta nazionale alla cibercriminalità spesso non può prescindere da una collaborazione a molteplici livelli. Essenziale a tal fine è la cooperazione internazionale rafforzata, in considerazione della natura internazionale e transfrontaliera del ciberspazio. La «Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro» è incentrata sulla creazione di un ciberspazio che promuova l'accesso a Internet e garantisca la crescita del mercato, ma mira anche a realizzare la ciberresilienza e a contrastare la cibercriminalità, trovando il giusto equilibrio tra i diritti fondamentali dei cittadini e lo Stato di diritto ([1]). Inoltre, promuove l'utilizzo di strumenti di cooperazione internazionale nella lotta contro la cibercriminalità nonché la cooperazione giudiziaria e di polizia in questo settore nei paesi terzi dai quali operano le organizzazioni cibercriminali ([2]).

Le conclusioni del Consiglio sulla comunicazione «Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE» ([3]) integrano la strategia dell'UE per la cibersicurezza evidenziando la necessità di prevenire, scoraggiare, individuare e contrastare le attività informatiche dolose. Inoltre, evidenziano l'esigenza di dotare le autorità pubbliche di strumenti atti a individuare, indagare e perseguire la cibercriminalità.

Eurojust si concentra sul contrasto della cibercriminalità nell'ottica di rafforzare la cooperazione giudiziaria in questo settore, in particolare favorendo una trattazione rapida delle richieste giudiziarie – un fattore cruciale per risolvere il problema della volatilità dei dati e colmare le lacune dovute all'applicazione di norme nazionali differenti in materia di conservazione dei dati – e il pronto coinvolgimento del potere giudiziario nelle operazioni di cibercriminalità, al fine di assicurare che, nella fase delle indagini, i dati siano raccolti in conformità delle norme applicabili e possano quindi essere considerati prove elettroniche ammissibili nei successivi procedimenti giudiziari. Eurojust realizza altresì prodotti strategici nel settore della cibercriminalità, o contribuisce significativamente alla loro realizzazione, aiutando in tal modo i professionisti competenti a sviluppare ulteriormente le competenze informatiche necessarie ([4]).

La presente relazione intende fornire una visione d'insieme dell'attività di Eurojust nel settore della cibercriminalità. Le operazioni svolte da Eurojust forniscono un'immagine accurata delle

([1]) Consiglio dell'Unione europea, conclusioni del Consiglio sulla comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza intitolata «Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro», Bruxelles, 22.7.2013 (12109/13).

([2]) Eurojust è impegnata in numerosi progetti per la creazione di capacità nel settore della cibercriminalità, quali il progetto Sirius (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), il progetto EuroMed Justice (https://www.euromed-justice.eu/) e il progetto GLACY+ (https://www.coe.int/en/web/cybercrime/glacyplus).

([3]) Consiglio dell'Unione europea, conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, Bruxelles, 20.11.2017 (14435/17).

([4]) Per maggiori informazioni cfr. la sezione «Pubblicazioni e progetti di Eurojust nel settore della cibercriminalità» del presente documento.

problematiche comuni che i professionisti del settore devono affrontare e delle buone prassi applicabili per risolverle. L'attività operativa di Eurojust costituisce un'utile fonte di informazioni sugli ostacoli specifici nel contesto della cooperazione giudiziaria e sui modi per superarli, alimentando la discussione su come affrontare al meglio il fenomeno della cibercriminalità. In un capitolo successivo sono forniti alcuni esempi di casi. Segue, infine, un elenco delle pubblicazioni interne e dei progetti di Eurojust rilevanti in materia di cibercriminalità.