Shrnutí

Existuje několik faktorů, které činí boj proti kyberkriminalitě jedinečným a náročným. Kyberkriminalita není ze své podstaty omezena hranicemi a rychle se vyvíjí, někdy rychleji, než na ni dokáží vnitrostátní orgány reagovat. Vzhledem k horizontálnímu charakteru kyberkriminality je tato problematika ještě složitější: na internetu dnes může docházet k téměř jakékoli formě trestné činnosti. Shromažďování elektronických důkazů takovéto trestné činnosti může být vzhledem k proměnlivosti údajů obtížné a může vyžadovat zvláštní odborné znalosti. Pro zajištění včasného uchování elektronických důkazů, což zaručuje jejich přípustnost v soudních řízeních, je zásadní justiční spolupráce. Mezinárodní justiční spolupráci mohou bránit značné rozdíly ve vnitrostátních právních rámcích (např. pokud jde o právní předpisy týkající se kriminalizace jednání či uchovávání údajů) a konflikty jurisdikcí. V důsledku nadnárodní povahy důkazů, které jsou nutné k úspěšnému stíhání pachatelů kybernetické trestné činnosti, fenomén kyberkriminality celkově přetváří tradiční právní pojetí zásady teritoriality.

Účinná vnitrostátní reakce na kyberkriminalitu proto často vyžaduje spolupráci na vícero úrovních. S ohledem na mezinárodní a přeshraniční charakter kyberprostoru má zásadní význam posílená mezinárodní spolupráce. „Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor“ se zaměřuje na vytvoření kyberprostoru, který podporuje přístup k internetu a zajišťuje růst trhu, ale usiluje také o dosažení kybernetické odolnosti a potírání kyberkriminality, přičemž se snaží nalézt správnou rovnováhu mezi základními právy občanů a právním státem ([1]). Podporuje rovněž využívání nástrojů mezinárodní spolupráce v boji proti kyberkriminalitě, jakož i související policejní a justiční spolupráci ve třetích zemích, z nichž organizace zapojené do kyberkriminality provozují svou činnost ([2]).

Závěry Rady o sdělení „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“ ([3]) doplňují strategii kybernetické bezpečnosti EU tím, že poukazují na nutnost předcházet nepřátelským činnostem v kyberprostoru, odrazovat od nich, odhalovat je a reagovat na ně. Zdůrazňují, že orgánům veřejné správy je třeba poskytnout nástroje k odhalování, vyšetřování a stíhání kyberkriminality.

Eurojust se zaměřuje na boj proti kyberkriminalitě s cílem posílit justiční spolupráci v této oblasti, zejména podporou rychlého vyřizování žádostí o justiční spolupráci (což je klíčový faktor v rámci řešení problematiky proměnlivosti údajů a odstraňování rozporů plynoucích z uplatňování různých vnitrostátních předpisů pro uchovávání údajů) a včasným zapojením justičních orgánů do operací v oblasti kyberkriminality, aby bylo zajištěno, že údaje jsou ve fázi vyšetřování shromažďovány v souladu s platnými předpisy, a mohou být tudíž v následných soudních řízeních předloženy jako přípustné elektronické důkazy. Eurojust navíc buď vytváří strategické produkty v oblasti kyberkriminality, nebo se na jejich tvorbě významně podílí, čímž pomáhá odborníkům z praxe dále rozvíjet nezbytné dovednosti týkající se kybernetické bezpečnosti ([4]).

Cílem této zprávy je poskytnout přehled činnosti Eurojustu v oblasti kyberkriminality. Operativní činnost Eurojustu umožňuje velmi dobře porozumět společným problémům odborníků z praxe a rovněž identifikovat osvědčené postupy k jejich překonání. Případy Eurojustu jsou užitečným zdrojem informací o konkrétních překážkách v souvislosti s justiční spoluprací a o tom, jak je lze překonat, a jsou podkladem pro diskusi o tom, jak nejlépe řešit problematiku kyberkriminality.

([1]) Rada Evropské unie, závěry Rady o společném sdělení Komise a vysoké představitelky Evropské unie pro zahraniční věci a bezpečnostní politiku nazvaném Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, Brusel, 22.7.2013 (12109/13).

([2]) Eurojust se účastní několika projektů budování kapacit v oblasti kyberkriminality, jako jsou projekty Sirius (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), EuroMed Justice (https://www.euromed-justice.eu/) a GLACY+ (https://www.coe.int/en/web/cybercrime/glacyplus).

([3]) Rada Evropské unie, závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU, Brusel, 20.11.2017 (14435/17).

([4]) Více informací naleznete v oddíle „Publikace a projekty Eurojustu v oblasti kyberkriminality“ tohoto dokumentu.

Následuje kapitola s příklady případů. Na závěr jsou uvedeny publikace a projekty Eurojustu, které jsou předmětem zájmu v oblasti kyberkriminality.