Zhrnutie

Boj proti počítačovej kriminalite je špecifický a náročný v dôsledku viacerých faktorov. Počítačová kriminalita vzhľadom na svoju povahu nepozná hranice a rýchlo sa vyvíja, pričom niekedy rýchlejšie, než vnútroštátne orgány dokážu reagovať. Ku komplexnosti počítačovej kriminality prispieva aj jej horizontálna povaha: takmer každý druh trestnej činnosti sa môže v súčasnosti vykonávať cez internet. Elektronické dôkazy takýchto trestných činov môže byť vzhľadom na nestálosť údajov ťažké zhromažďovať a môžu si vyžadovať osobitné odborné znalosti. Zabezpečenie včasného uchovania elektronických dôkazov, aby boli prípustné v súdnych konaniach, si vyžaduje justičnú spoluprácu. Medzinárodnej justičnej spolupráci môžu brániť výrazné rozdiely vo vnútroštátnych právnych rámcoch (napr. týkajúcich sa kriminalizácie konania alebo právnych predpisov o uchovávaní údajov) a spory o právomoc. Celý fenomén počítačovej kriminality pretvára tradičnú právnu koncepciu zásady teritoriality v dôsledku nadnárodnej povahy dôkazov potrebných na zabezpečenie úspešného stíhania páchateľov počítačovej kriminality.

Účinná vnútroštátna reakcia na počítačovú kriminalitu si preto často vyžaduje spoluprácu na viacerých úrovniach. Kľúčom je posilnenie medzinárodnej spolupráce, keďže kybernetický priestor má medzinárodnú a cezhraničnú povahu. Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor sa zameriava na vytvorenie kybernetického priestoru, ktorým sa podporuje prístup na internet a zabezpečuje rast trhu, pričom jeho cieľom je dosiahnuť kybernetickú odolnosť a bojovať proti počítačovej kriminalite, čím sa dosiahne správna rovnováha medzi základnými právami občanov a zásadou právneho štátu ([1]). Okrem toho podporuje využívanie nástrojov medzinárodnej spolupráce v boji proti počítačovej kriminalite, ako aj súvisiacu policajnú a justičnú spoluprácu v tretích krajinách, z ktorých svoju činnosť vykonávajú zločinecké organizácie pôsobiace v oblasti počítačovej kriminality ([2]).

Závery Rady o spoločnom oznámení: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ ([3]) dopĺňajú stratégiu kybernetickej bezpečnosti EÚ zdôraznením potreby predchádzať škodlivým kybernetickým činnostiam, odrádzať od nich, odhaľovať ich a reagovať na ne. V záveroch sa zdôrazňuje, že subjektom verejného sektora sa musia poskytnúť nástroje na odhaľovanie, vyšetrovanie a stíhanie počítačovej kriminality.

Eurojust sa zameriava na boj proti počítačovej kriminalite s cieľom posilniť justičnú spoluprácu v tejto oblasti, najmä uľahčovaním rýchleho vybavovania súdnych žiadostí – čo je kľúčový faktor pri riešení otázky nestálosti údajov a odstraňovaní rozdielov vyplývajúcich z uplatňovania rôznych vnútroštátnych pravidiel uchovávania údajov – a včasným zapojením súdnictva do operácií v oblasti počítačovej kriminality s cieľom zabezpečiť, aby sa počas fázy vyšetrovania údaje zhromažďovali v súlade s platnými pravidlami a na základe toho sa mohli predkladať v následných súdnych konaniach ako prípustné elektronické dôkazy. Okrem toho Eurojust buď produkuje strategické produkty v oblasti počítačovej kriminality, alebo k nim významne prispieva, čím pomáha odborníkom z praxe ďalej rozvíjať potrebné zručnosti v oblasti počítačovej kriminality ([4]).

Táto správa poskytuje prehľad o práci agentúry Eurojust v oblasti počítačovej kriminality. Operačná práca, ktorú agentúra Eurojust vykonáva, ponúka podrobný prehľad o spoločných výzvach, ktorým čelia odborníci z praxe, ako aj o najlepších postupoch na prekonanie týchto výziev. Práca agentúry

([1]) Rada Európskej únie, Závery Rady o spoločnom oznámení Komisie a vysokej predstaviteľky Európskej únie pre zahraničné veci a bezpečnostnú politiku: Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor, Brusel, 22. 7. 2013 (12109/13).

([2]) Agentúra Eurojust sa angažuje v niekoľkých projektoch zameraných na budovanie kapacít v oblasti počítačovej kriminality, ako je projekt Sirius (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), projekt EuroMed Justice (https://www.euromed-justice.eu/) a projekt GLACY+ (https://www.coe.int/en/web/cybercrime/glacyplus).

([3]) Rada Európskej únie, Závery rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ, Brusel, 20. 11. 2017 (14435/17).

([4]) Viac informácií sa nachádza v časti „Eurojust's publications and projects in the area of cybercrime" (Publikácie a projekty agentúry Eurojust v oblasti počítačovej kriminality)" tohto dokumentu.

Eurojust na prípadoch je užitočným zdrojom informácií o konkrétnych prekážkach v kontexte justičnej spolupráce a o tom, ako ich možno prekonať, čo prispieva k diskusii o najlepších riešeniach javu počítačovej kriminality. V ďalšej kapitole sú uvedené príklady prípadov. A napokon správa obsahuje publikácie agentúry Eurojust a projekty jej záujmu v oblasti počítačovej kriminality.