Sukces i porażka w śledztwach dotyczących cyberprzestępczości: czynniki kryminologiczne i procesowe

Cyberprzestępczość to powszechne i trwałe zagrożenie. Każdego dnia w sieci popełniane są przestępstwa — od włamań i ataków z użyciem złośliwego oprogramowania, przez oszustwa, po mowę nienawiści i inne nadużycia w mediach społecznościowych. Większość z tych czynów nigdy nie zostaje wykryta. Wiele z nich nie jest nawet zgłaszanych organom ścigania. Jednak nawet gdy pokrzywdzeni decydują się zawiadomić organy ścigania, postępowania często kończą się niepowodzeniem z powodu nieustalenia sprawcy. Spośród dużej liczby przestępstw popełnianych w cyberprzestrzeni tylko niewielka część kończy się skutecznym wykryciem i doprowadzeniem sprawcy do odpowiedzialności karnej — istnieje zatem swoista „luka" w egzekwowaniu prawa wobec cyberprzestępczości. Dlaczego niektóre śledztwa kończą się sukcesem, a inne nie?

Celem niniejszego projektu badawczego jest odpowiedź na to pytanie. Projekt opiera się na analizie rzeczywistych akt spraw karnych z sądów i prokuratur aby zidentyfikować czynniki, które sprzyjają skuteczności śledztw lub ją utrudniają. Zespół badawczy przeanalizuje postępowania z dwóch punktów widzenia: działań podejmowanych przez organy ścigania oraz strategii działania sprawców. Naszym celem jest ustalenie, czy istnieją statystycznie istotne różnice w taktykach śledczych lub takie działaniach sprawców pomiędzy sprawami zakończonymi wniesieniem aktu oskarżenia a tymi, które zostały umorzone z powodu niewykrycia sprawcy. Tego rodzaju wiedza może być użyteczna przy projektowaniu przyszłych szkoleń, interwencji legislacyjnych i działań prewencyjnych.

Projekt wykorzystuje mieszaną metodologię badawczą, łącząc metody ilościowe i jakościowe. Chcemy poddać analizie reprezentatywną próbę prawomocnie zakończonych spraw karnych z różnych rejonów sądowych w Polsce (umorzonych i zakończonych sądowo). Z każdej sprawy pozyskamy zanonimizowane dane dotyczące wybranych czynników — określonych na podstawie literatury i konsultacji z ekspertami z zakresu informatyki śledczej i przedstawicielami zawodów prawniczych. Zgromadzone dane zostaną poddane analizie statystycznej, obejmującej m.in. regresję logistyczną i modele drzew decyzyjnych, w celu identyfikacji czynników — takich jak np. rodzaje dowodów, decyzje procesowe czy warunki działania sprawców — które są najsilniej powiązane z sukcesem lub porażką śledztwa. Równolegle przeprowadzimy analizę jakościową wybranych spraw, tworząc tzw. skrypty opisujące typowe sposoby popełnienia czynu oraz przebieg śledztwa. Takie podejście pomoże w projektowaniu skuteczniejszych działań zapobiegawczych. Porównamy również wyjaśnienia podejrzanych z głównymi teoriami kryminologicznymi, aby zidentyfikować wzorce motywacji i schematy podejmowania decyzji.

Choć badanie osadzone jest w polskim kontekście jurysdykcyjnym, poruszane w nim problemy — takie jak szyfrowanie danych, anonimowość w sieci czy współpraca z platformami internetowymi — mają charakter uniwersalny. Wyniki projektu będą istotne dla badaczy, praktyków prawa oraz decydentów poszukujących skuteczniejszych sposobów reagowania na cyberprzestępczość.

Projekt nie ma charakteru aplikacyjnego ani technicznego. Nie zakłada opracowywania nowych narzędzi ani procedur śledczych. Jego celem jest pogłębienie wiedzy naukowej na temat przebiegu typowych postępowań dotyczących cyberprzestępstw, zidentyfikowanie czynników wpływających na ich rezultat oraz sformułowanie wniosków wynikających z rzeczywistej praktyki. Wyniki zostaną udostępnione w otwartych publikacjach naukowych, podczas konferencji i w publicznie dostępnych raportach. Dzięki analizie rzeczywistych spraw — a nie tylko analizie teoretycznej czy przedstawieniu statystyk — projekt ten ma na celu dostarczenie praktycznej i użytecznej wiedzy, która może przyczynić się do poprawy skuteczności ścigania cyberprzestępczości w Polsce i na świecie.