Waldemar Jaroch

KRYMINALISTYCZNE ASPEKTY WSPÓŁCZESNEJ PRZESTĘPCZOŚCI GOSPODARCZEJ (zagadnienia wybrane)

Wprowadzenie

Przestępczość gospodarcza jest jednym z najbardziej złożonych problemów społecznych, które można rozpatrywać w rożnych aspektach, w tym prawnokarnym, kryminologicznym, kryminalistycznym. Poszczególne rodzaje przestępstw ulegają permanentnym zmianom wraz ze zmianą warunków gospodarowania. Nowe formy przestępstw wypierają tradycyjną przestępczość gospodarczą. Brak definicji ustawowej przestępstwa gospodarczego oraz oparcie się na zakreśleniu zjawisk określanych jako przestępczość gospodarcza poprzez wskazanie konkretnych przestępstw powoduje, iż część z nich traci swą aktualność, przeobrażając się często w nowe formy przestępne, wymagające nowych technik wykrywczych i dokumentacyjnych pod względem kryminalistycznym[1]. Wydaje się, iż nie ma powodów, by dyskutować o problemach określania, czym właściwie jest lub czym może być przestępczość gospodarcza. W świetle natomiast nowoczesnych technik i technologii, wynikających z postępu technicznego, istnienia środków szybkiej komunikacji oraz nowoczesnych form kontaktów gospodarczych (komunikacja przez Internet) należy zwrócić uwagę na zagrożenia szczególnymi rodzajami przestępstw, jak np. przestępstwa teleinformatyczne, komputerowe.

Proces wykrywczy przestępstw gospodarczych jest szczególnie utrudniony właśnie z uwagi na bardzo dynamiczny postęp technologii komputerowych, środków komunikowania się i anonimowego nawiązywania transakcji, co daje sprawcom przestępstw szerokie możliwości przestępczego działania.

Obserwuje się także zmianę jakościową w działalności zorganizowanych grup przestępczych, które preferują obecnie zorganizowaną działalność gospodarczą, a nie kryminalną. Według danych Centralnego Biura Śledczego

[1] Przykład wskazanych w Katalogu przestępstw gospodarczych Rady Europy m.in. przestępstw komputerowych, następnie cyberprzestępczość.

w strukturze grup przestępczych dominują grupy narkotykowe (147 grup w 2008 r., 121 grup w 2007 r., 85 grup w 2006 r.), ale zaraz na następnej pozycji są grupy ekonomiczne (131 w 2008 r., 118 grup w 2007 r., 88 grup w 2006 r.).[2] Można powiedzieć, że polskie gangi polubiły gospodarkę.

W szczególności chodzi o wykazywane przez sprawców zainteresowanie giełdami papierów wartościowych czy zjawiskiem tzw. prania pieniędzy. W tym kontekście nie bez znaczenia pozostaje obowiązująca w tym zakresie procedura karna, a w szczególności określone w niej możliwości zabezpieczenia i uzyskiwania dowodów z komputerowych nośników informacji. Wielokrotnie problemem w skutecznym ściganiu sprawców przestępstw teleinformatycznych jest anonimowość użytkowników (np. kawiarenek internetowych). Oczywiście, komunikacja między podmiotami (bank – klient, giełda) jest zabezpieczana najnowocześniejszymi systemami ochrony, szyfrowania i detekcji włamań, ale i techniki przestępne „nadążają" za postępem w tym zakresie.

Problematyka metod wykrywczych

Pytaniem zasadniczym w aspekcie kryminalistycznym jest pytanie o metody i ich skuteczność w wykrywaniu przestępstw gospodarczych. W ciągu ostatnich lat w wielu krajach znacznie zwiększyła się liczba międzynarodowych badań empirycznych na temat przestępstw gospodarczych, w tym na temat sposobów i metod ich wykrywania. Stosowane (wykorzystywane) sposoby i metody zarówno wykrywania, jak i zapobiegania przestępczości gospodarczej są właściwe (adekwatne do prowadzonej działalności) dla podmiotów gospodarczych, które we własnym interesie ekonomicznym zainteresowane są maksymalnym ograniczeniem nadużyć gospodarczych. Najbardziej właściwym środkiem ustalania tych sposobów i metod jest opinia samych przedsiębiorców. Oczywiście, należy mieć na uwadze ten element, że dotyczy to głównie określonej grupy przestępstw, na które są narażone te podmioty[3].

Badania Pricewaterhouse i wydziału prawa na Martin-Luther-University[4]

Najczęściej wskazywane przestępstwa to sprzeniewierzenie aktywów (w Polsce 80%, w świecie 62%), w następnej kolejności oszustwo (w Polsce 56%, w świecie 47%), korupcja jako trzecia w Polsce (19%), w świecie jako trzecie piractwo i podrabianie (25%), piractwo i podrabianie w Polsce czwarte (13%), w świecie następne w kolejności to korupcja i fałszowanie danych finan-

2 Zob. Raporty Centralnego Biura Śledczego.

3 Inna sytuacja będzie miała miejsce w stosunku do przestępstw przeciwko interesowi fiskalnemu państwa czy przestępstw przeciwko kontroli państwa nad produkcją i konsumpcją.

4 Wyniki badań firmy PricewatershauseCooper oraz Uniwersytetu im. M. Lutra w Halle z 2005 r.: badaniom poddano 3634 respondentów (członkowie zarządów, prawnicy, audytorzy wewnętrzni, specjaliści ds. zarządzania ryzykiem), w tym 101 respondentów z Polski.

sowych (po 24%), fałszowanie danych finansowych piąte w Polsce (11%), wykorzystanie informacji poufnych do obrotu akcjami w Polsce na szóstej pozycji (4%), w świecie pranie brudnych pieniędzy (7%), pranie brudnych pieniędzy w Polsce jako kolejne (1%), w świecie natomiast jako kolejne wykorzystanie informacji poufnych do obrotu akcjami (4%)[5]

Z przeprowadzonych badań wynika, że najskuteczniejszą metodą wykrywczą tej grupy przestępstw jest audyt wewnętrzny lub zewnętrzny (w Polsce 32% spółek wskazuje na audyt, w świecie - 28%), następnie - wewnętrzne lub zewnętrzne doniesienia (analogicznie: w Polsce - 16%, w świecie aż 28%), systemy bezpieczeństwa korporacyjnego (w Polsce – 16%, w świecie – tylko 4%), przypadek (w Polsce – 3%, w świecie – 6%), inne (w Polsce – 26%, w świecie – 18%)[6]. Co charakterystyczne, na audyt wskazuje się jako na najskuteczniejszą metodę zarówno w Polsce, jak i w świecie. Następnym źródłem informacji o przestępstwach są wewnętrzne i zewnętrzne doniesienia oraz w Polsce – systemy bezpieczeństwa korporacyjnego.

Z kolei wśród metod zapobiegania nadużyciom wskazuje się:

1) audyt wewnętrzny (87%),
2) audyt zewnętrzny (85%),
3) kontrole wewnętrzne (79%),
4) informacje publiczne (65%),
5) kodeksy etyczne (52%),
6) systemy bezpieczeństwa korporacyjnego (48%),
7) konsultacje dotyczące zapobiegania (42%),
8) zarządzanie ryzykiem (32%),
9) specjalne testy rekrutacyjne (31%),
10) szkolenia dotyczące nadużyć (30%)[7].

Nie bez znaczenia dla procesu wykrywczego i stosowanych metod wykrywczych oraz zapobiegania przestępstwom pozostaje problematyka sprawców przestępstw gospodarczych, a w szczególności ich relacje (związek) z firmą. Z badań międzynarodowych wynika, że w tej kategorii przestępstw połowa sprawców była pracownikami oszukanej firmy, a niemal jedna czwarta należała do wyższego kierownictwa. W Polsce relacje te były korzystniejsze pod względem liczby pracowników firmy, bowiem jedynie jedna trzecia dokonujących przestępstwa była pracownikami firmy, natomiast mniej korzystne są dane, jeśli chodzi o członków kierownictwa, bowiem aż 45% pracowników-przestępców w Polsce stanowiło najwyższe kierownictwo.

5 Badania firmy PricewatershauseCooper oraz Uniwersytetu im. M. Lutra w Halle.

6 Tamże.

7 Tamże.

Aspekt ekonomiczny przestępczości

Aspekt ekonomiczny to przede wszystkim aspekt strat na skutek przestępstwa. Z przedstawionych badań wynika, że na świecie średni koszt finansowy nadużyć wynosił 1,74 mln USD na jedną spółkę. W Polsce średnie straty firmy będące efektem nadużycia były zdecydowanie niższe, gdyż wyniosły prawie 460 tys. USD. Aspekt ekonomiczny to także wpływ na organizację oraz pośredni wpływ na reputację i markę firmy, morale i motywacje pracowników, relacje biznesowe oraz wartość akcji/udziałów. Pawie 30% badanych firm uznało, że poniesione straty finansowe miały poważny bądź bardzo poważny wpływ na ich organizację.

Odzyskiwanie strat

Istotną kwestią jest także problematyka odzyskiwania strat poniesionych w wyniku nadużyć. Z badań wynika, że w Polsce odzyskano 40% strat, w tym 20% w przedziale do 60% poniesionych strat i 20% powyżej 60%. W świecie relacje te przedstawiały się następująco: odzyskano 47% strat, w tym 20% w przedziale do 60% poniesionych strat i 27% powyżej 60%. Relacje w tym zakresie są zatem podobne.

Badania firmy Deloitte[8]

Z kolei badania prowadzone przez firmę Deloitte wskazują, iż najczęstszym sposobem wykrywania nadużyć są rutynowe działania nadzorcze kierownictwa (70% wskazań w 2004 r. i 66% w 2003 r.), informacje od pracownika (43% w 2003 r. i 42% w 2004 r.), audyt wewnętrzny (42% w 2003 r. i 31% w 2004 r.), przypadek (21% w 2003 r. i 20% w 2004 r.), anonimowa informacja (17% w 2004 r., w 2003 r. brak danych), organy ścigania (8% w 2003 r. i 7% w 2004 r.), system zarządzania ryzykiem (13% w 2003 r. i 6% w 2004 r.), audyt zewnętrzny (6% w 2003 r. i 4% w 2004 r.), inny sposób (7% w 2003 r. i 3% w 2004 r.). Według badanych najgroźniejsze nadużycia gospodarcze to łapownictwo i korupcja (82% badanych wskazywało w 2003 r. i 86% w 2004 r.), przestępczość zorganizowana (62% w 2003 r. i 62% w 2004 r.), sprzeniewierzenie majątku firmy (43% w 2003 r. i 39% w 2004 r.), fałszowanie sprawozdań finansowych (23% w 2003 r. i 32% w 2004 r.), pranie brudnych pieniędzy (27% w 2003 r. i 19% w 2004 r.), przestępstwa komputerowe (6% w 2003 r. i 8% w 2004 r.). Natomiast już wśród wewnętrznych nadużyć gospodarczych

[8] Badania sondażowe firmy Deloitte we współpracy z Bankiem Światowym i International Business Leaders Forum. Celem badań było zapoznanie się z opiniami na temat postrzegania nadużyć gospodarczych, a także poznanie stanu wiedzy o nich i procesów kontroli mających te nadużycia ograniczać. Wyjściową próbę badawczą stanowiło dwa tysiące największych działających w Polsce przedsiębiorstw wyłonionych na podstawie rankingu dziennika „Rzeczpospolita". Spośród dwóch tysięcy wysłanych ankiet odesłanych zostało 238.

wskazuje się na pierwszym miejscu sprzeniewierzenie majątku przez pracownika (40%), nieuzasadnione zakupy (33%) prywatne zakupy za pieniądze firmy (28%), łapówkarstwo (20%), konflikt interesów (17%), kradzież informacji (16%), nieuprawnione wykorzystywanie komputerów (15%), fałszowanie faktur (15%), nepotyzm w rekrutacji pracowników (13%), sfałszowanie sprawozdania finansowego (4%), pranie brudnych pieniędzy (1%), inne (1%)[9].

W problematyce zapobiegania przestępczości gospodarczej, jak też wykrywania konkretnych przestępstw istotne pozostają poszczególne sfery (działy) działalności gospodarczej, w których najczęściej odnotowuje się przestępczość. Z badań wynika, że najczęściej przestępstwa odnotowuje się w działach: sprzedaży (54% respondentów wskazało na tę sferę działalności w 2003 r. i 49% w 2004 r.), zaopatrzenia (41% w 2003 r. i 42% w 2004 r.), marketingu (18% w 2003 r. i 13% w 2004 r.), produkcji (12% w 2003 r., ale 22% w 2004 r.), finansach (14% w 2003 r. i 13% w 2004 r.)[10].

W opinii ankietowanych najczęściej za popełnienie nadużyć odpowiedzialni są pracownicy (67%), na drugim miejscu znaleźli się menedżerowie niższego szczebla (23%), następnie dostawcy (21%), menedżerowie wyższego szczebla (20%), klienci (18%), agenci i przedstawiciele nie będący pracownikami (15%), urzędnicy publiczni (7%), firmy konkurencyjne (6%), inne osoby (2%)[11].

Wśród postrzeganych konsekwencji nadużyć gospodarczych wskazywano na obniżenie morale pracowników (51%), osłabienie reputacji firmy (23%), utratę kontrahentów (15%), utratę zaufania akcjonariuszy (7%), inne skutki (14%)[12].

Według badań tylko 7% badanych podmiotów wskazało na organy ścigania jako sposób wykrycia przestępstwa gospodarczego.

Skuteczność wykrywcza przestępstw gospodarczych zależy od wielu czynników, ale podstawowym, wręcz fundamentalnym niewątpliwie są możliwości prawnego działania. Należy zwrócić uwagę na fakt, że wiele rozwiązań prawnych w zakresie wprowadzanych instrumentów zwalczania przestępczości gospodarczej nie spełniało oczekiwań praktyków, gdyż zawierało liczne, można powiedzieć fundamentalne, ograniczenia. Przykładem kontrolowane wręczenie lub przyjęcie korzyści majątkowej (tzw. łapówka kontrolowana)[13] ograniczone było zastrzeżeniem, że czynności te nie mogą polegać na nakłanianiu bądź

9 Dane dotyczą roku 2004.

10 Procenty nie sumują się do 100, gdyż respondenci mogli wskazać więcej niż jedną odpowiedź.

11 Dane dotyczą roku 2004.

12 Dane dotyczą także 2004 r.

13 Wprowadzona ustawą z 21 lipca 1995 r. o zmianie ustaw: o urzędzie Ministra Spraw Wewnętrznych, o Policji, o Urzędzie Ochrony Państwa, o Straży Granicznej oraz niektórych innych ustaw (Dz.U. Nr 104, poz. 515).

kierowaniu tego rodzaju przedsięwzięciem.[14] Podobnie, jeżeli chodzi o dostęp organów policji do danych objętych tajemnicą bankową czy ubezpieczeniową na etapie czynności operacyjno-rozpoznawczych. Jak można więc skutecznie zwalczać i zapobiegać przestępczości na szkodę tych instytucji, gdy niemożliwe było uzyskanie podstawowych danych w przedmiocie chociażby ustalenia, czy dana osoba (podejrzewana o przestępstwo) jest stroną umowy? Dopiero z czasem ograniczenia te zostały usunięte przez ustawodawcę.[15] Także przepisy regulujące sposoby przeciwdziałania praniu pieniędzy wprowadzone ustawą z 16 listopada 2000 r.[16] obowiązujące od 23 czerwca 2001 r. nie w pełni wprowadziły wszystkie instrumenty, w tym zasadnicze. Wielokrotnie nowelą do ustawy przesuwano termin wejścia w życie obowiązku rejestracji transakcji przekraczających wartości progowe (art. 8) oraz obowiązku informowania generalnego inspektora informacji finansowej o tych transakcjach (art. 11). Przepisy te weszły ostatecznie w życie z dniem 1 lipca 2004 r.

Niestety, nadal wiele kwestii w tym zakresie pozostaje co najmniej dyskusyjne w sensie legislacyjnym, biorąc pod uwagę dążenie do zapewnienia skutecznego wykrywania i zapobiegania przestępczości gospodarczej. Artykuł 20 ust. 3 ustawy o Policji[17] stanowi na przykład, że jeżeli jest to konieczne dla skutecznego zapobieżenia przestępstwom określonym w art. 19 ust. 1 tej ustawy lub ich wykrycia albo ustalenia sprawców i uzyskania dowodów, Policja może korzystać z informacji dotyczących umów ubezpieczenia, a w szczególności z przetwarzanych przez zakłady ubezpieczeń danych podmiotów, w tym osób, które zawarły umowę ubezpieczenia, a także przetwarzanych przez banki informacji stanowiących tajemnicę bankową. Obwarowanie tego przepisu trybem warunkowym „jeżeli jest to konieczne dla skutecznego zapobieżenia przestępstwom" oraz złożona procedura udostępnienia tego rodzaju informacji z uwagi na to, że informacje takie mogą być udostępnione na podstawie postanowienia wydanego na pisemny wniosek Komendanta Głównego Policji albo komendanta

[14] Ograniczenia te zostały zniesione z dniem 19 marca 2002 r. ustawą z 27 lipca 2001 r. o zmianie ustawy o Policji, ustawy o działalności ubezpieczeniowej, ustawy – Prawo bankowe (Dz.U. Nr 100, poz. 1084).

[15] Uprawnienia uzyskiwania informacji objętych tajemnicą bankową i ubezpieczeniową przed wszczęciem postępowania karnego zostały przyznane z dniem 19 marca 2002 r. ustawą z 27 lipca 2001 r. o zmianie ustawy o Policji i niektórych innych ustaw (Dz.U. Nr 100, poz. 1084).

[16] Ustawa z 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł (Dz.U. Nr 116, poz. 1216); obecnie ustawa z 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz przeciwdziałaniu finansowaniu terroryzmu (j.t. Dz.U. z 2003 r. Nr 153, poz. 1505 z późn.zm.).

[17] Ustawa z 6 kwietnia 1990 r. o Policji (j.t. Dz. U. z 2002 r. Nr 7, poz. 58 z późn.zm.); powoływana jako „ustawa o Policji".

wojewódzkiego Policji przez sąd okręgowy właściwy miejscowo ze względu na siedzibę wnioskującego organu (art. 20 ust. 5) – ograniczają w znacznym stopniu operatywność działania organów, które z mocy ustawy powołane są do zapobiegania i zwalczania tego rodzaju przestępczości.

Także rozwiązania, przyjęte ustawą o Policji w zakresie kontroli operacyjnej (art. 19) nasuwają określone zastrzeżenia, biorąc pod uwagę aktualne zagrożenia przestępczością zorganizowaną o charakterze transnacjonalnym (pranie pieniędzy, przestępczość narkotykowa, wyłudzenia z tytułu podatku VAT i inne).

Kontrola operacyjna, głównie w postaci stosowania podsłuchu z uwagi na złożoność proceduralną (zarządza sąd okręgowy w drodze postanowienia na wniosek Komendanta Głównego Policji po uzyskaniu zgody Prokuratora Generalnego bądź na wniosek komendanta wojewódzkiego Policji po uzyskaniu pisemnej zgody właściwego miejscowo prokuratora okręgowego) wydaje się już obecnie nie w pełni odpowiadać potrzebom praktyki. Zwłaszcza że w stosunku do pozostałych metod szczególnych, jak operacja „przesyłki niejawnie nadzorowanej" wystarczające jest zawiadomienie właściwego prokuratora okręgowego czy też w przypadku „zakupu kontrolowanego" – zgoda właściwego prokuratora okręgowego.[18]

Należy przy tym podkreślić, iż podobne wymogi proceduralne dotyczą także pozostałych służb, jak Straż Graniczna, ABW, kontrola skarbowa itd.

W proponowanych rozwiązaniach należałoby mieć na uwadze skrócenie drogi w procesie decyzyjnym, aby zapewnić funkcjonalność i skuteczność działania organów w zwalczaniu przestępczości. Odrębną kwestią pozostaje zwiększenie kontroli prokuratorskiej czy sądowej, ale jest to wykonalne pod względem legislacyjnym i praktycznym.

Ściganie oszustw internetowych wymaga pilnych nowelizacji[19]

W strukturze przestępczości gospodarczej dominują oszustwa. Wzrost liczby przestępstw popełnianych z wykorzystaniem Internetu, a zwłaszcza oszustw na portalach aukcyjnych jest znaczny i zdaje się uzasadniać nowelizację obowiązujących przepisów. Analiza dotychczasowych regulacji wskazuje na potrzebę weryfikacji i modyfikacji. Postulatem *de lege ferenda* jest niewątpliwie wprowadzenie do procedury karnej możliwości zastosowania podsłuchu w sprawach o oszustwa internetowe na podstawie przepisów rozdziału 26 kodeksu postępowania karnego[20] oraz rozszerzenie katalogu przestępstw wymienionych w art. 237 § 3 k.p.k., w których wypadku możliwe byłoby stosowanie podsłuchu treści przekazów informacji czy też rozmów telefonicznych, prowadzonych

[18] Zob. art. 19a i 19b ustawy o Policji.

[19] M. Jachimowicz, *Która prokuratura, za pomocą jakich instrumentów*, Rzeczpospolita z 12.08.2006 r.

[20] Tytuł rozdziału: *Kontrola i utrwalanie rozmów*.

przez sprawców zarówno pomiędzy sobą, jak i z potencjalnymi pokrzywdzonymi[21]. Podsłuch taki powinien obejmować również bieżącą kontrolę transakcji internetowych zawieranych przez sprawców oraz wszelkie inne czynności w sieci związane z uprawianym procederem (np. dokonywanie przelewów bankowych), co umożliwiłaby w razie zmiany regulacja art. 241 k.p.k.[22] W chwili obecnej możliwe jest jedynie, na podstawie art. 218 k.p.k., uzyskiwanie w czasie rzeczywistym danych dotyczących obiegu informacji. Przepis art. 218 k.p.k. daje sądowi oraz prokuratorowi, na żądanie zawarte w postanowieniu, możliwość uzyskiwania wykazu połączeń telekomunikacyjnych od urzędów, instytucji oraz podmiotów prowadzących działalność w dziedzinie poczty lub działalność telekomunikacyjną, który informuje o czasie połączenia oraz innych kwestiach zawiązanych z nim, ale nie informuje o treści rozmowy telefonicznej. Na tej podstawie uzyskiwane są przez organa ścigania m.in. bilingi telefoniczne. Przepis ten nie wymienia danych abonenta wskazanego numeru telefonicznego, które umożliwiają jego identyfikację (imię, nazwisko, miejsce zamieszkania), gdyż są objęte tajemnicą telekomunikacyjną i wyraźnie oddzielone od danych identyfikujących połączenie (art. 159 ustawy – Prawo telekomunikacyjne[23]).

Wskazany wyżej przepis proceduralny wśród podmiotów zobowiązanych do wydania korespondencji oraz przesyłek nie wymienia usługodawców świadczących usługi drogą elektroniczną. Chodzi tu o doprecyzowanie treści art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną[24].

Przepis ten stanowi, że usługodawca udziela informacji o danych dotyczących użytkownika i wykorzystanych przez niego usługach organom państwa na potrzeby prowadzonych przez nie postępowań, ale – jak zauważono – jest to przepis o charakterze odsyłającym.

Konieczna jest również o wiele większa ostrożność banków w procedurze zawierania umów dotyczących otwarcia rachunku bankowego, zwłaszcza w aspekcie wykorzystywania struktur banków do procederu prania brudnych pieniędzy. Obecnie można zrobić to bez osobistego kontaktu.

Podkreślić należy szczególnie groźne zagrożenia, jakie powoduje przestępstwo *phishingu*, polegające na wyłudzaniu poufnych informacji osobistych, tzw. danych wrażliwych dotyczących loginów, haseł, szczegółów rachunku bankowego, karty kredytowej itp. Jest to rodzaj ataku opartego na inżynierii społecznej – socjotechnice. Termin wprowadzony w połowie lat 90. przez *cracerów* próbujących wykraść konta użytkowników serwisu pocztowego AOL. Metoda

21 M. Jachimowicz, op. cit.

22 Tamże; art. 241 k.p.k.: Przepisy tego rozdziału (26) stosuje się odpowiednio do kontroli oraz do utrwalania przy użyciu środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną.

23 Dz.U. z 2004 r. Nr 171, poz. 1800 z późn.zm.

24 Dz.U. z 2002 r. Nr 144, poz. 1204 z późn.zm.

działania jest bardzo prosta i najczęściej polega na rozsyłaniu do przypadkowych osób wiadomości, w których sprawcy podszywają się pod pracowników działów bezpieczeństwa lub informatyzacji konkretnego banku, wyłudzając w ten sposób dane wrażliwe. Innym sposobem jest podstawienie strony internetowej, identycznej, jaką posługuje się bank.

Z proponowanych rozwiązań należałoby też rozważyć rozszerzenie katalogu przestępstw, w związku z którymi banki będą podawały dane osobowe posiadaczy kont bez uprzedniej konieczności uruchamiania procedury zwolnienia z tajemnicy bankowej.

Wnioski

Dynamiczny postęp technologiczny w zakresie przetwarzania i przesyłu informacji, nawiązywania i realizowania transakcji handlowych, operacji finansowych wymaga odpowiednich zmian i dostosowań legislacyjnych na gruncie czynności operacyjno-rozpoznawczych, procedury karnej, jak i karno-materialnej.

Dotychczasowe doświadczenia wskazują na syndrom „spóźnionego prawa", czyli prawa jako spóźnionego sojusznika w zwalczaniu zorganizowanej przestępczości gospodarczej. Nieznane są zatem rzeczywiste straty ekonomiczne dla państwa, a w konsekwencji dla społeczeństwa. Jedynie antycypowanie zagrożeń pod względem ustawodawczym i odpowiednie wyposażanie organów w prawne instrumenty zwalczania, jak i uwzględnienie w porę doświadczeń innych państw w tym zakresie może w konsekwencji ograniczyć zjawisko „niskiej wykrywalności" przestępstw gospodarczych.

Zmiana struktury własnościowej w okresie transformacji spowodowała przeniesienie ciężaru w sferze podmiotowo-kompetencyjnej w zakresie zwalczania przestępczości gospodarczej. Proces ten trwa również obecnie. Zasadniczym pytaniem jest pytanie o to, kto i w jakim zakresie zajmować się ma zwalczaniem i wykrywaniem przestępstw gospodarczych. Czy w tym zakresie główny ciężar spada na podmioty bezpośrednio prowadzące działalność gospodarczą? Przykładowo na właścicieli spółek, instytucje rynku finansowego, jak banki, zakłady ubezpieczeń, giełdy itp. Czy też państwo ma szczególny obowiązek zapewnić bezpieczeństwo ekonomiczne wszystkim podmiotom i w równym stopniu poprzez swoje agendy i organy prowadzić aktywną działalność w zakresie wykrywania przestępstw? Jeżeli tak, to konieczna jest strategia zwalczania tej przestępczości.

Ustawodawca konsekwentnie nakłada zadania w zakresie zwalczania i zapobiegania przestępczości, gdzie tylko to możliwe, natomiast rzeczywistość pozostaje rzeczywistością, czyli mamy do czynienia ze stosunkowo niską wykrywalnością przestępstw.

Skuteczne zwalczanie przestępczości gospodarczej zależy też od systemu i struktury administracji ekonomicznej i kontroli, a także wymaga dobrego ich funkcjonowania. Niewydolność któregoś z tych systemów powoduje, że znacząca liczba przestępstw gospodarczych nie zostanie wykryta.