CYBERTERRORYZM W PRAWIE KARNYM MATERIALNYM - PRZYCZYNEK DO DYSKUSJI NA GRUNCIE ANALIZY DOGMATYCZNEJ

ADAM BAWOROWSKI, ADW.

Autor wskazuje na problemy dotyczące rozumienia pojęcia terroryzmu w aktach prawnych i analizuje podstawy prawne penalizacji czynów o charakterze terrorystycznym w polskim Kodeksie karnym. Wskazuje jednocześnie na niejednolitość nazewnictwa opisującego przestępstwa dotyczące przetwarzania danych i informacji w systemach informatycznych i teleinformatycznych. Niekonsekwencje terminologiczne ustawodawcy przedstawione zostały jako główny problem w ściganiu i karaniu sprawców przestępstw o charakterze terrorystycznym. W artykule podjęta została również próba zdefiniowania pojęcia cyberterroryzmu oraz wskazania wniosków *de lege ferenda* pozwalających na urealnienie ścigania tego typu czynów zabronionych, w tym zmiany definicji legalnej przestępstwa o charakterze terrorystycznym.

W dniu 9 marca 2009r. Rada Ministrów przyjęła Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Dokument ten zakłada, iż „z uwagi na wzrost zagrożeń ze strony sieci publicznych (…), a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, niezbędne jest skoordynowanie działań w zakresie zapobiegania i zwalczania cyberterroryzmu, które umożliwią szybkie i efektywne reagowanie na zagrożenia i ataki wymierzone przeciwko krytycznym systemom i sieciom teleinformatycznym", nieodzownym jest wdrożenie działań prawnych, organizacyjnych, technicznych i edukacyjnych zapobiegających i zwalczających te zagrożenia[1].

Działania organizacyjno-prawne mają przejawiać się między innymi w zdefiniowaniu pojęć dotyczących cyberprzestępczości i cyberterroryzmu. Właśnie tych zagadnień będzie dotyczyła niniejsza praca.

Omawiany dokument określił, iż cele z niego wypływające będą zrealizowane w latach 2009-2011. A zatem w tym czasie musi dojść do stworzenia definicji legalnych wielu pojęć dotyczących cyberprzestrzeni. Nie jest to zadanie łatwe, a to z co najmniej dwóch przyczyn. Po pierwsze szybki rozwój techniki informatycznej i elektronicznej powoduje powstawanie coraz to nowszych możliwości przetwarzania informacji, trudnych do szybkiego wprowadzenia w ramy prawne z uwagi na długotrwały proces legislacyjny. Przykładem może tu być przepis art. 267§1 kk w brzmieniu sprzed nowelizacji wprowadzonej Ustawą z dnia 24 października 2008r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz.U. nr 214 poz. 1344) „…kto … podłącza się do przewodu…". Dopiero zatem pod koniec 2008r. ustawodawca spenalizował podłączenie się do sieci telekomunikacyjnej, tym samym przewidując karalność przechwycenia informacji przesyłanej przez medium bezprzewodowe. Lecz należy zauważyć, iż już na początku tego wieku sieci bezprzewodowe istniały i działały.

Drugą przyczyną utrudniającą wprowadzenie do porządku prawnego definicji jest niejednolitość nazewnictwa dotyczącego omawianej sfery. Nie jest to tylko prawa polskiego, ale co ważniejsze, prawa międzynarodowego. Bowiem gdy spojrzymy na Konwencje Rady Europy dostrzeżemy używanie tych samych określeń opisujących inne sytuacje prawne oraz nazywanie tych samych pojęć co rusz innym mianem.

Dla porządku, rozważania nad zakresem karalności cyberterroryzmu w polskim prawie karnym należy rozpocząć od wskazania, jak rozumiane jest pojęcie terroryzmu.

Potocznie terroryzmem jest to „pojęcie najczęściej definiowane jako użycie siły lub przemocy przeciwko osobom lub własności z pogwałceniem prawa, mające na celu zastraszenie i wymuszenie na danej grupie ludności lub państwie ustępstw w drodze do realizacji określonych celów. Działania terrorystyczne mogą dotyczyć całej populacji, jednak najczęściej są one uderzeniem w jej niewielką część, aby pozostałych obywateli zmusić do odpowiednich zachowań"[2].

W nauce kryminologii terroryzm jest rozumiany niejednolicie. Wskazuje się, iż mimo wzmożenia działalności terrorystycznej na świecie, nie wypracowano jednolitej koncepcji definicji terroryzmu[3].

Równocześnie w traktatach i umowach międzynarodowych traktujących o terroryźmie nie znajdujemy definicji terroryzmu. Jedynie preambuły tych dokumentów odnoszą się do tego pojęcia, nie precyzując go, a nadto uznają za terrorystyczne wyliczone w nich przestępstwa.

Dla przykładu można podać, iż Konwencja Rady Europy o zapobieganiu terroryzmowi, sporządzona w Warszawie dnia 16 maja 2005 r. i ratyfikowana przez Rzeczpospolitą Polską (Dz. U. 2008 nr 161 poz. 998) stanowi, iż przestępstwo o charakterze terrorystycznym oznacza każde przestępstwo pozostające w zakresie i zdefiniowane w jednym z traktatów wymienionych w Załączniku i są to:

1) Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, sporządzona w Hadze dnia 16 grudnia 1970 r.;

---

[1] http://cert.gov.pl/images/stories/form/Zalozenia_Rzadowy_Program_Ochrony_Cyberprzestrzeni_RP_2009-2011.pdf, s. 4

[2] http://pl.wikipedia.org/wiki/Terroryzm

[3] B. Hołyst, Terroryzm, LexisNexis, Warszawa 2009, Tom 1, s. 52

2) Konwencja o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, sporządzona w Montrealu dnia 23 września 1971 r.;
3) Konwencja o zapobieganiu przestępstwom i karaniu sprawców przestępstw przeciwko osobom korzystających z ochrony międzynarodowej, w tym przeciwko dyplomatom, sporządzona w Nowym Jorku dnia 14 grudnia 1973 r.;
4) Międzynarodowa konwencja przeciwko braniu zakładników, sporządzona w Nowym Jorku dnia 17 grudnia 1979 r.;
5) Konwencja o ochronie fizycznej materiałów jądrowych, przyjęta w Wiedniu dnia 3 marca 1980 r.;
6) Protokół o zwalczaniu bezprawnych czynów przemocy w portach lotniczych obsługujących międzynarodowe lotnictwo cywilne uzupełniający Konwencję o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego podpisaną w Montrealu dnia 23 września 1971 r., sporządzony w Montrealu dnia 24 lutego 1988 r.;
7) Konwencja w sprawie przeciwdziałania bezprawnym czynom przeciwko bezpieczeństwu żeglugi morskiej, sporządzona w Rzymie dnia 10 marca 1988 r.;
8) Protokół w sprawie przeciwdziałaniu bezprawnym czynom przeciwko bezpieczeństwu stałych platform umieszczonych na szelfie kontynentalnym, sporządzony w Rzymie dnia 10 marca 1988 r.;
9) Międzynarodowa konwencja o zwalczaniu terrorystycznych zamachów bombowych, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 grudnia 1997r.;
10) Międzynarodowa Konwencja o zwalczaniu finansowania terroryzmu, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r.

W polskim Kodeksie karnym legalna definicja nie określa co to jest terroryzm, a wskazuje jedynie na charakter przestępstwa – „przestępstwo o charakterze terrorystycznym". Inne przepisy tej Ustawy odnoszą się do tej definicji.

By można mówić o przestępstwie o charakterze terrorystycznym muszą być spełnione następujące przesłanki:

- czyn zabroniony musi być zagrożony karą pozbawienia wolności w wysokości co najmniej 5 lat,

oraz

- musi być popełniony w jednym z poniższych celów:
  1) poważnego zastraszenia wielu osób,
  2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
  3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej - a także groźba popełnienia takiego czynu.

Najważniejszym czynnikiem wyznaczającym terrorystyczny charakter czynu jest zatem zamiar sprawcy, zawsze bezpośredni znamienny celem. Nie każdy jednak czyn popełniony w celu określonym w tym przepisie będzie miał charakter terrorystyczny. Czyn ten bowiem musi być zagrożony karą co najmniej 5 lat pozbawienia wolności. Cenzus ten skutecznie zatem ogranicza zakres czynów zabronionych, które mogą posiadać omawiany charakter.

Udowodnienie sprawcy, iż popełnił on przestępstwo o charakterze terrorystycznym skutkuje dla niego wyższą odpowiedzialnością karną, na podstawie art. 65 kk. Wyższa karalność tego typu czynów będzie też wynikała z przepisu art. 258 §2 i 4 kk.

Kodeks karny wprowadza również zasadę, iż ustawę tę stosuje się do obywatela polskiego (art. 109 kk) oraz cudzoziemca (art. 110§1 kk), który popełnił czyn o charakterze terrorystycznym poza granicami Polski. Jednakże karalność takiego czynu będzie wymagała, zgodnie z przepisem art. 111§1 kk, warunku podwójnej karalności, co oznacza, iż w miejscu popełnienia tego czynu przestępstwo o charakterze terrorystycznym musi być również karane. Jak zauważył A. Marek, ustawodawca niepotrzebnie zawęził możliwość ścigania i ukarania sprawcy, bowiem tą regulacją wyłączył stosowanie przepisu art. 113 kk, który pozwala na ściganie na mocy umów międzynarodowych w przypadku braku podwójnej karalności czynu[4].

Innym aktem normatywnym, w którym można poszukiwać definicji terroryzmu jest Ustawa z dnia 16 listopada 2000r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (tekst jednolity Dz. U. 2003 nr 153 poz. 1505 z pózn. zm.). Jednak mimo użytego w jej tytule słowa terroryzm, nie definiuje się tam tego pojęcia. W art. 2 pkt 7 wprowadza się za to definicję aktu terrorystycznego, którym są przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne, przestępstwa przeciwko bezpieczeństwu powszechnemu oraz przestępstwa określone w art. 134 i 136 Kodeksu karnego. Jak widać zdefiniowanie aktu terrorystycznego ma zupełnie inną budowę normatywną niż definicja przestępstwa

[4] A. Marek, Kodeks karny. Komentarz, LEX, 2007, wyd. IV.

o charakterze terrorystycznym ujęta w art. 115§20 kk. Ustawodawca zawęził krąg czynów mogących mieć charakter aktu terrorystycznego do wyliczonych w komentowanym przepisie. Nadto przesądzono, iż każdy czyn ujęty w przepisach art. 117-126 kk (Rozdział XVI Przestępstwa przeciwko pokojowi, ludzkości oraz przestępstwa wojenne), art. 163-172 kk (Rozdział XX Przestępstwa przeciwko bezpieczeństwu powszechnemu) oraz art. 134 i 136 kk jest aktem terrorystycznym, choć tak w rzeczywistości być nie musi. Zauważyła to Rada Ministrów, bowiem w Rządowym programie ochrony cyberprzetsteni RP na lata 2009-2011 czytamy: „szczególnie często zdarzenia pozornie o charakterze terrorystycznym okazują się być zdarzeniami o charakterze ledwie kryminalnym. Zdarza się również, iż działania pierwotnie uznane za kryminalne okazują się być fragmentem skorelowanych działań o większej skali bądź poważniejszych skutkach”[5].

Równocześnie do definicji nie włączono wielu istotnych czynów zabronionych, które mogą mieć charakter terrorystyczny. Dla ilustracji dość wspomnieć o przestępstwach przeciwko obronności, które z definicji mogą zagrażać newralgicznym dla Państwa interesom i wśród których znajduje się art. 140 kk – „Kto, w celu osłabienia mocy obronnej Rzeczypospolitej Polskiej, dopuszcza się gwałtownego zamachu na jednostkę Sił Zbrojnych Rzeczypospolitej Polskiej, niszczy lub uszkadza obiekt albo urządzenie o znaczeniu obronnym, podlega karze pozbawienia wolności od roku do lat 10”.

Podkreślić należy, iż z puli cyberprzestępstw *sensu stricte*, w zakresie objętym aktem terrorystycznym znalazł się tylko czyn penalizowany w art. 165 kk. Faktem jest, iż wszystkie przestępstwa z wyliczonych w art. 2 pkt 7 Ustawy z dnia 16 listopada 2000r. wypełniają warunek formalny definicji przestępstwa o charakterze terrorystycznym, bowiem są zagrożone karą pozbawienia wolności co najmniej 5 lat, jednakże nie może to przesądzać o charakterze tych czynów. Wynikiem tej definicji będzie obowiązek spoczywający na instytucjach zobowiązanych informowania Generalnego Inspektora Informacji Finansowej o transakcjach, co do których istnieje uzasadnione podejrzenie, że mają związek z popełnianiem przestępstw w niej wyliczonych, choćby te czyny w sensie prawnokarnym nie miały charakteru terrorystycznego. *A contrario* takiego obowiązku nie ma, gdy zajdzie podejrzenie, że transakcje mają związek z innymi przestępstwami, nie wyliczonymi w definicji aktu terrorystycznego, chociażby spełniały one warunki definicji z art. 115§20 kk. Zdziwienie musi budzić fakt, iż banki, jako instytucje zobowiązane do informowania GIIF o podejrzanych transakcjach mogących mieć związek z aktem terrorystycznym, nie mogą powiadomić o atakach na ich infrastrukturę, bowiem definicja zawarta w art. 2 pkt 7 Ustawy nie wylicza tego typu przestępstw.

Dodać także wypada, iż niedostosowanie definicji aktu terrorystycznego z komentowanej ustawy do definicji przestępstwa o charakterze terrorystycznym z art. 115§20 kk przejawia się w tym, iż Kodeks karny wskazuje na czyn godzący w gospodarkę Rzeczypospolitej Polskiej lub innego państwa, co zostało pominięte w cytowanym art. 2 pkt 7 Ustawy.

Dla rozwiązania zaistniałej sytuacji prawnej można podać dwa warianty postępowania legislacyjnego.

Po pierwsze, na gruncie Kodeksu karnego można uznać, iż przestępstwa wyliczone w art. 2 pkt 7 ustawy z dnia 16 listopada 2000r. posiadają w każdym wypadku walor charakteru terrorystycznego lub, po drugie, inkorporować do tejże Ustawy definicję z art. 115§20 kk.

Pierwszy wariant wydaje się nie do przyjęcia, bowiem stworzyłby fikcję prawną eliminującą kryminalny charakter wyliczonych przestępstw. Drugie rozwiązanie jest warte rozważenia, bowiem wprowadzałoby tożsamość rozumienia pojęć, na dobrą sprawę, takich samych i czyniłoby zadość zasadzie jednolitości systemu prawnego.

Jednakże należy zadać pytanie, czy aby definicja przyjęta w art. 115§20 kk odpowiada potrzebom dnia dzisiejszego?

By udzielić odpowiedzi należy najpierw nakreślić, chociażby schematycznie, obiekty i sposoby ataków cyberterrorystycznych i dokonać ich analizy prawnokarnej.

W dzisiejszej dobie obiekty, które mogą podlegać atakom terrorystycznym można podzielić na dwa rodzaje: materialne i niematerialne. Do materialnych zaliczymy budynki, urządzenia oraz ludzi, do niematerialnych zaś informacje i dane.

Ataki na obiekty materialne są w literaturze przedmiotu opisane i scharakteryzowane w sposób pełny. Jednakże nie jest tak w przypadku ataków na informacje i dane, zatem należy rozwinąć to zagadnienie, bowiem to właśnie one w zasadniczej mierze będą stanowić cel działania sprawców. Ogólnie rzecz ujmując, będą to zarówno ataki na przekazy niosące treści mogące mieć konkretne znaczenie dla odbiorcy, np. instrukcje postępowania, jak i przekazy w formie danych będących w istocie komendami dla urządzeń.

W rozumieniu karnoprawnym pojęcia informacji i danych są rozumiane niejednolicie oraz, co należy podkreślić, istnieją pomiędzy nimi istotne różnice[6].

---

[5] http://cert.gov.pl/images/stories/form/Zalozenia_Rzadowy_Program_Ochrony_Cyberprzestrzeni_RP_2009-2011.pdf, s. 10

[6] A. Adamski, Prawo karne komputerowe, C.H.Beck Warszawa 2000, s. 37 i n.

Dane to „przedstawienie faktów, pojęć lub poleceń w sposób sformalizowany i umożliwiający ich komunikowanie, interpretację lub przetwarzanie, zarówno przez ludzi, jak i urządzenia". Informacja zaś jest to „znaczenie, jakie nadajemy danym przy pomocy konwencji odnoszących się do tych danych"[7].

Zatem dane mogą być źródłem informacji lub jej nośnikiem.

Powyższe rozróżnienie ma niebagatelne znaczenie prawne. Mamy bowiem do czynienia z przestępstwami dotyczącymi informacji *sensu stricte* – art. 265 – 269b kk zebranymi w Rozdziale XXXIII Przestępstwa przeciwko ochronie informacji, jak też innymi przepisami, które penalizują jedynie przetwarzanie danych – art. 165kk, art. 287kk. Wskazać należy w tym miejscu na pewną niekonsekwencję ustawodawcy, który dane traktuje na równi z informacją, na co wskazywać może umieszczenie w Rozdziale XXXIII Kodeksu karnego czynów skierowanych przeciwko danym – art. 268a kk, 269 kk oraz 269a kk.

Podział na dane i informacje ma również znaczenie dla opisania innej sytuacji – mianowicie czynów przestępnych skierowanych na przetwarzanie danych w systemach lub sieciach informatycznych i teleinformatycznych. Poczynić bowiem należy następne istotne zastrzeżenie. Jak ustalono powyżej rozumienie treści informacji uzależnione jest od jej odbiorcy. Zatem informacja musi być przedstawiona w sposób dla niego znany i przyjęty. Dane zaś są wykorzystywane jako nośnik informacji, ale też instrukcje i komendy dla systemów przetwarzających je.

Dochodzimy więc do istotnej konstatacji: podstawą dla działania systemów informatycznych są dane, które przez nie są przetwarzane i mogą być przesyłane za pośrednictwem systemów teleinformatycznych.

Powyższe rozróżnienie między informacją a danymi zdaje się dostrzegać ustawodawca penalizujący szereg działań nakierowanych na systemy i sieci, ale tu dochodzimy do znaczącej niekonsekwencji legislacyjnej.

Analiza zapisów Kodeksu karnego oraz Ustaw: z dnia 24 października 2008r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Dz.U. nr 214 poz. 1344), z dnia 4 września 2008r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej **(**Dz.U. nr 171 poz. 1056), z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zwanej dalej ustawą o informatyzacji (Dz. U. Nr 64, poz. 565, z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501 oraz z 2008 r. Nr 127, poz. 817), Ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144 poz. 1204 z pózn. zm.) oraz z dnia 16 lipca 2004r. prawo telekomunikacyjne (Dz.U. nr 171 poz. 1800) wskazuje na prawnie niejednolite rozumienie pojęcia systemów przetwarzających dane w poszczególnych ustawach, a nawet w obrębie jednej z nich – Kodeksie karnym.

Zgodnie z postanowieniem art. 62 Ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne ustawodawca wprowadził zmiany w szeregu aktów normatywnych Ustawą z dnia 4 września 2008r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej **(**Dz.U. nr 171 poz. 1056) zwana dalej ustawą ujednolicającą. Wprowadza ona w wielu ustawach jednolite rozumienie określeń: „informatyczny nośnik danych", „dokument elektroniczny", „system teleinformatyczny" oraz „środki komunikacji elektronicznej". Po zmianie dokonanej w wyliczonych tam ustawach, w tym Kodeksie karnym, powyższe terminy mają być rozumiane tak jak wyrażenia wymienione w art. 3 pkt 1-4 ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zwanej dalej ustawą o informatyzacji (Dz. U. Nr 64, poz. 565, z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501 oraz z 2008 r. Nr 127, poz. 817).

Niestety do Kodeksu karnego wprowadzono tylko jedno ujednolicenie – „informatyczny nośnik danych". Zatem cel Ustawy jakim było ustandaryzowanie terminologii informatycznej nie został do końca osiągnięty. Co więcej omawiana ustawa wprowadziła wiele kontrowersji w rozumieniu znamion czynów z art. 267§2 kk, 269a kk, 269b kk.

Ilustracją tego stanu rzeczy niech będzie wprowadzenie przez ustawę ujednolicającą do porządku prawnego (oprócz Kodeksu karnego) pojęcia „system teleinformatyczny" i jednoczesne pozostawienie w Kodeksie karnym przez ustawodawcę określeń: „system komputerowy", „sieć teleinformatyczna", „system informatyczny".

Analiza dogmatyczna takiego rozwiązania pozwala na wyprowadzenie następującego wniosku: jako że „system teleinformatyczny" zgodnie z definicją legalną Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. nr 144 poz. 1204 z pózn. zm.) obejmuje zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z 2001 r. Nr 122, poz. 1321 i Nr 154, poz. 1800 i 1802 oraz z 2002 r. Nr 25, poz. 253 i Nr 74, poz. 676) to do przesyłania danych nie służą:

1. systemy informatyczne (art. 267§2 kk)

[7] Ibidem, s. 38-39, Recommendatoin of the Council of the OECD concerning Guidelines for the Security of Information System, OECD/GD (92) 10 Paris, 1992

2. systemy komputerowe (art. 269a kk i 269b kk), co ewidentnie nie było zamysłem ustawodawcy, a nawet jest przeciwstawne jego celowi[8]. Jednakże przy dokonywaniu wykładni przepisów prawa karnego materialnego pierwszeństwo ma wykładnia językowa przed wykładnią celowościową.

Na marginesie należy jednocześnie wskazać na niedbałość legislacyjną, ponieważ ustawa z dnia 21 lipca 2000r. - Prawo telekomunikacyjne zastąpiona została Ustawą z dnia 16 lipca 200 r. Prawo telekomunikacyjne.

Jak z powyższego wynika istnieje potrzeba ponownego zdefiniowania pojęć dotyczących informatyki i informatyzacji w odniesieniu do Kodeksu karnego. Dopiero te ustalenia pozwolą na wypracowanie definicji odnoszących się do cyberterroryzmu.

Jednakże, na gruncie obecnego stanu prawnego można pokusić się o stwierdzenie, iż zasadniczym polem działania sprawców ataków terrorystycznych związanych z informatyką będą systemy przetwarzające i przesyłające dane.

Modus operandi sprawców może być różny, od prostych działań na wybrane urządzenia i oprogramowanie, których celem będzie wyłączenie lub spowolnienie ich procesów, do złożonych czynności, które pojedynczo nie będą stanowiły przestępstwa, ale będą prowadziły do jego popełnienia.

Przykładem prostego działania o charakterze terrorystycznym będzie przeprowadzenie tzw. ataku DoS lub DDoS. „DoS (ang. ***D**enial of **Service)*** jest to atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. DDoS (ang. ***D**istributed **D**enial of **S**ervice*), przeprowadzany równocześnie z wielu komputerów (np. zombie) i jest odmianą ataku DoS z tą różnicą, że polega na jednoczesnym atakowaniu ofiary z wielu miejsc. Służą do tego najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej ilości żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu”[9].

Powyższe czyny zakwalifikować można jako przestępstwa z art. 268§2 kk w zakresie naruszenia prawa do zapoznania się z informacją, z art. 268§1 kk w zakresie utrudniania dostępu do danych, jak też zakłócania lub uniemożliwiania automatycznego przetwarzania, gromadzenia lub przekazywania danych, z art. 269 kk w zakresie zakłócania lub uniemożliwiania automatycznego przetwarzania, gromadzenia lub przekazywania danych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, z art. 269a kk w zakresie zakłócenia w istotnym stopniu pracy systemu komputerowego lub sieci teleinformatycznej. Dyspozycja art. 165§1 pkt 4 kk również zostanie wypełniona działaniem sprawcy, który zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych sprowadza niebezpieczeństwo dla życia i zdrowia wielu osób lub mienia w wielkich rozmiarach[10].

Podkreślić należy, iż tylko przestępstwa z art. 165§1 pkt 4 i 269§1 kk będą mogły być zakwalifikowane jako o charakterze terrorystycznym, bowiem ich zagrożenie karą wynosi co najmniej 5 lat.

Jednakże każdy z powyżej przytoczonych czynów zabronionych może *de facto* przybrać postać terrorystyczną, bowiem ataki na przetwarzanie danych mogą dotyczyć takich newralgicznych sektorów jak służba zdrowia, energetyka, telekomunikacja, gazownictwo lub bankowość. Te części gospodarki narodowej nie zostały ujęte w przepisach art. 164§1 pkt 4 kk i 269§1 kk, a zatem przestępcze skierowane na nie działania nie będą mogły być ścigane i karane jako przestępstwa o charakterze terrorystycznym.

Ze złożonym działaniem na przetwarzanie danych będziemy mieli do czynienia w przypadku wykonywania wielu czynności przestępnych przeciwko danym, informacjom oraz przetwarzającym je urządzeniom i oprogramowaniu.

Dla przykładu można tu przedstawić pokrótce mechanizm tzw. phishingu bankowego, którego celem jest kradzież pieniędzy klientów banków internetowych.

Zjawisko to polega na uzyskaniu przez sprawców dostępu do konta klienta banku, uzyskaniu kodów jednorazowych pozwalających na dokonanie transakcji, dokonanie operacji przelania pieniędzy na inne, kontrolowane przez sprawców konto bankowe i przekazanie pieniędzy w postaci gotówki, najczęściej poza

---

[8] Według ustawodawcy przepis art. 267§2 kk ma penalizować właśnie zachowania przestępne popełniane przez sieć telekomunikacyjną – z uzasadnienia: „Czyn taki może polegać np. na wprowadzeniu do systemu informatycznego oprogramowania, które umożliwia sprawcy przejęcie zdalnej kontroli nad komputerem, w celu wykonania z jego wykorzystaniem zmasowanych ataków na określone strony internetowe”.

[9] http://pl.wikipedia.org/wiki/DDoS

[10] Wyliczenia form czynności sprawczych, które *de facto* odnoszą się do przetwarzania danych, które są użyte w cytowanych przepisach nie są najszczęśliwszym zabiegiem legislacyjnym. Jak widać zakresy te w różnych przepisach krzyżują się, doprowadzając do zamętu przy stosowania prawa. Należałoby się zatem zastanowić nad przyjęciem definicji przetwarzania danych zawartej w art. 7 pkt 2 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

granice RP. W opisanym procederze bierze udział szereg wyspecjalizowanych „komórek” działających na rzecz sprawców, niejednokrotnie składających się z osób, które nie wiedzą, że uczestniczą w czynie zabronionym.

Praktycznie rzecz biorąc, w opisanym przypadku mamy do czynienia z następującymi czynnościami:

1. nabór osób, które założą konta bankowe, na które następnie zostaną przelane pieniądze pochodzące z kradzieży;
2. produkcja złośliwych programów mających na celu przejęcie komputerów do własnych celów oraz przechwycenie danych dotyczących logowania się do konta bankowego;
3. rozsyłanie złośliwego oprogramowania („zarażanie komputerów”);
4. logowanie się do konta bankowego z komputerów zainfekowanych złośliwym oprogramowaniem bez wiedzy ich właścicieli;
5. dokonywanie przelewów na podstawione konta bankowe;
6. wypłacenie gotówki przez podstawione osoby i przesłanie jej poza granice RP;
7. pobranie gotówki przez podstawione osoby.

Jak zatem widać do skutku przestępnego wejścia w posiadanie pieniędzy innej osoby dochodzi poprzez wykonanie wielu czynów zabronionych. Mamy tu do czynienia m. in. z przestępstwami określonymi w art. 269b kk (produkcja programów służących do popełniania przestępstw), 269a kk (infekowanie komputerów), 267§2 kk (nieuprawniony dostęp do systemu informatycznego), 278§1 kk (kradzież), 292 i 293 kk (paserstwo pieniędzy).

Powyższe przestępstwa są popełniane przeciwko osobom fizycznym, ale też przeciwko systemom banków, bowiem ingerencja w postaci zmiany danych zachodzi w ich infrastrukturze informatycznej.

Powyżej zarysowany proceder może mieć charakter czysto kryminalny, bez cech terroryzmu, ale też może służyć jego finansowaniu. Niestety Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu nie uznaje takich czynów za akty terrorystyczne.

W tym miejscu należy wspomnieć o przeoczeniu legislacyjnym jakim jest brak wprowadzenia do polskiego porządku prawnego przestępstwa tzw. rekrutacji na rzecz terroryzmu, bowiem, jak pokazano na przykładzie, szereg ataków na systemy wymaga udziału wielu wyspecjalizowanych „komórek”.

Obowiązek penalizacji rekrutacji na rzecz terroryzmu wynika wprost z art. 6 Konwencji Rady Europy o zapobieganiu terroryzmowi, sporządzonej w Warszawie dnia 16 maja 2005r. i ratyfikowanej przez RP (Dz. U. 2008 nr 161 poz. 998). W tym przepisie wprowadza się definicję takiej rekrutacji - namawianie innej osoby do popełnienia lub uczestniczenia w popełnieniu przestępstwa o charakterze terrorystycznym lub też do przystąpienia do zrzeszenia lub grupy w celu przyczynienia się do popełnienia jednego lub więcej przestępstw o charakterze terrorystycznym przez to zrzeszenie lub grupę.

Trudno przecenić siłę Internetu przy rekrutowaniu nowych członków organizacji terrorystycznych, ponieważ rozwój tego medium jest stale postępujący[11] oraz uznawany jest za zapewniający bezpieczeństwo komunikowania się oraz anonimowość. Bezpieczeństwo komunikowania przejawia się m. in. w wielu możliwościach kryptograficznych nadawania komunikatów, a anonimowość w używaniu tzw. komputerów przesiadkowych (proxy), których celem jest zatarcie śladów działalności.

Zatem należy postulować szybkie wprowadzenie do Kodeksu karnego nowego typu przestępstwa rekrutacji na rzecz terroryzmu.

Wspomniana Konwencja nakłada również na strony obowiązek penalizacji szkolenia na rzecz terroryzmu (art. 7) oraz publicznego nawoływania do popełnienia przestępstwa o charakterze terrorystycznym (art. 5). Te czyny również można popełnić przy użyciu techniki informatycznej. Internet jako medium publiczne, nie posiadające żadnej cenzury, doskonale nadaje się do upubliczniania wszelkich informacji.

Ostatnim przepisem, który powinien być wprowadzony do Kodeksu karnego na podstawie komentowanej Konwencji, jest „nieistotność popełnienia przestępstwa o charakterze terrorystycznym”. Regulacja ta sankcjonuje więc istniejącą potrzebę penalizacji działań, które mogą prowadzić do popełnienia przestępstwa o charakterze terrorystycznym. Jednakże należy zgłosić uwagę, iż nie tylko te zachowania ułatwiają dokonanie czynu o zabarwieniu terrorystycznym, o czym była mowa poprzednio.

W obowiązującej Ustawie Kodeks karny przygotowanie do przestępstwa o charakterze terrorystycznym nie jest karalne. Karalne jest jedynie przygotowanie do poszczególnych przestępstw, które mogą mieć charakter terrorystyczny, ale mogą być także przestępstwami czysto kryminalnymi.

Z uwagi na fakt, iż warunkiem formalnym dla zaistnienia omawianego charakteru przestępstwa jest jego zagrożenie karą co najmniej 5 lat, krąg tych przestępstw jest wąski. Jednak, jak wykazano wyżej, na czyn o charakterze terrorystycznym może składać się szereg działań, które brane każde z osobna nie są

[11] Według danych GUS 48% gospodarstw domowych w Polsce posiada dostęp do internetu, http://media2.pl/internet/44165-dostep-do-internetu-ma-48-proc.-gospodarstw-domowych.html

przestępstwami o wysokiej karalności, ale każde z nich może stanowić swoiste przygotowanie i prowadzić do popełnienia innego przestępstwa o charakterze terrorystycznym.

Zatem dochodzimy znowu do konstatacji, iż większość przestępstw skierowanych przeciwko informacjom, danym i systemom je przetwarzającym, *de facto* mogących posiadać przymiot terroryzmu, nie będzie mogła być uznana i ścigana jako terrorystyczne.

Mając powyższe ustalenia na względzie należy powrócić do definicji przestępstwa o charakterze terrorystycznym ustalonej art. 115§20 kk i dokonać próby dostosowania jej do przestępstw przeciwko informacjom, danym oraz systemom je przetwarzającym.

Jak widać, warunek formalny zagrożenia karą w wysokości co najmniej 5 lat nie jest do utrzymania. Sprawia on bowiem, iż większość czynów dotyczących sfery informatyki nie jest ścigana i karana w trybie przestępstwa o charakterze terrorystycznym.

Zatem, aby umożliwić realne przeciwdziałanie terroryzmowi można podjąć działania legislacyjne dwojakiego rodzaju. Po pierwsze można podwyższyć zagrożenie karą tego typu przestępstw, aby uczynić zadość definicji z art. 115§20 kk. Drugim wariantem jest zrezygnowanie w tej definicji z warunku co najmniej pięcioletniego zagrożenia karą.

Druga ze wskazanych możliwości wydaje się możliwą do zrealizowania, bowiem nie będzie zgodne z zasadami polityki karnej i legislacji podwyższanie istniejących kar za przestępstwa *stricto* kryminalne. Dodatkowo można pokusić się o wprowadzenie do prawa karnego karalności przygotowania do przestępstwa o charakterze terrorystycznym, co pozwoli uniknąć zbędnej kazuistyki kryminalizującej poszczególne znamiona czynności sprawczej. Ten postulat jest o tyle na miejscu, że postęp informatyki jest trudny do przewidzenia, a zatem niemożliwy do opisania w przepisach, które powinny być w miarę ogólnie sformułowane.

Poczynienie powyższych ustaleń pozwala na podjęcie próby sprecyzowania pojęcia cyberterroryzmu w ramach prawa karnego materialnego.

Punktem wyjścia jest stwierdzenie, iż działania sprawców w zakresie ataków informatycznych nakierowane są na dane, informacje oraz systemy przetwarzające te dane. System składa się z urządzeń oraz programów przystosowanych do przetwarzania danych, w tym ich przechowywania i przesyłania. Przechowywanie danych jest domeną systemów informatycznych, a przesyłanie systemów teleinformatycznych. Biorąc pod uwagę legalną definicję systemu teleinformatycznego, która zawiera w sobie też opisanie systemu informatycznego, należy uznać, że w pełni oddaje ona meritum zagadnienia.

Sprawcy będą posługiwali się zdalnym dostępem (poprzez sieć Internet) do przedmiotu czynności sprawczej, ale też mogą działać fizycznie na urządzenia lub ich części, a nawet na ludzi obsługujących te urządzenia oraz programy. Te wszystkie działania będą miały związek z informatyką, a ściślej z przetwarzaniem informacji, choć czasami mogą nie dotykać sfery czysto technicznej.

Zatem można już wytłumaczyć pojęcie „cyber". Określenie to jest pierwszym członem wyrazów złożonych wskazujący na ich związek z informatyką, a zwłaszcza z Internetem[12]. Czyli cyberprzestępczością będzie przestępczość związana z informatyką, a cyberterroryzm będzie odmianą terroryzmu związaną z informatyką, a zwłaszcza z siecią Internet. Majac więc na uwadze definicję z art. 115§20 kk dochodzimy do wniosku, iż cyberterroryzmem będzie przestępne działanie związane z informatyką i mające jeden z poniższych celów:

1) poważnego zastraszenia wielu osób,

2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,

3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej - a także groźba popełnienia takiego czynu.

Ograniczeniem formalnym ścigania cyberterroryzmu jest wymóg karalności w wymiarze co najmniej 5 lat pozbawienia wolności.

Na koniec niniejszych uwag należy sformułować w sposób skondensowany wnioski *de lege ferenda.*

Dla skutecznego ścigania cyberterroryzmu w pierwszym rzędzie trzeba wprowadzić jednolite nazewnictwo informatyczne w całym systemie prawa polskiego, a w szczególności w systemie prawa karnego. Nie może być bowiem tak, że przepisy opisujące w rzeczywistości te same pojęcia posługują się innymi nazwami. Za punkt wyjścia do prac w tym temacie można zaproponować Ustawę z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz.U. nr 171 poz. 1056). Ujednolicenie nazewnictwa będzie czynić zadość zasadzie określoności ustawowego opisu przestępstwa.

Następnym wnioskiem jest potrzeba dostosowania definicji zawartej w art. 115§20 kk do specyfiki zasad penalizacji i polityki karnej dotyczących przestępstw skierowanych na przetwarzanie danych i informacji. Dopasowanie to powinno mieć formę rezygnacji z warunku formalnego minimalnej karalności przestępstwa o charakterze terrorystycznym.

Również ujednolicenie definiowania charakteru terrorystycznego czynu zabronionego pomiędzy różnymi ustawami jest niezbędnie potrzebne dla uczynienia zadość zasadzie jednolitości systemu prawnego.

---

[12] Słownik Języka Polskiego, http://sjp.pwn.pl/

Nadto należałoby pochylić się nad potrzebą wprowadzenia karalności przygotowania do popełnienia przestępstwa o charakterze terrorystycznym.

Na koniec warto wnieść uwagę ogólną, związaną z możliwościami skutecznego ścigania cyberterroryzmu przez funkcjonariuszy do tego powołanych. Otóż, z uwagi na fakt, iż materia cyberprzestępczości stanowi *novum* w systemie prawa oraz wkracza bardzo głęboko w sferę techniczną działania systemów przetwarzających dane, niezbędnym zdaje się wdrożenie kompleksowych zasad nauczania i szkolenia w tym zakresie funkcjonariuszy odpowiednich służb oraz prawników, a w szczególności prokuratorów, których obowiązkiem jest strzeżenie praworządności i nadzór nad ściganiem przestępstw. Nie ulega bowiem kwestii, iż bez przygotowania merytorycznego wykonywanie tych ustawowych zadań będzie tylko pozornym wypełnianiem powinności Państwa wobec swoich Obywateli.

CYBERTERRORISM IN CRIMINAL LAW – A CONTRIBUTION TO THE DISCUSSION ON THE BASIS OF DOGMATIC ANALYSIS

Summary

The author indicates the problems concerning the understanding of the concept of terrorism in legal acts and analyses the legal basis of penalizing terrorist acts in Polish penal code. Moreover, the author shows the inconsistency of terminology that describes the offences concerning data and information processing in computer systems. The inconsistency of terminology of the legislator is shown as the major problem in prosecuting and penalizing perpetrators of the offences of terrorist nature.

The author also tries to define the notion of cyberterrorism as well as to present proposals *de lege ferenda* (one of them being an attempt to change the legal definition of a terrorist act) that would allow to prosecute such offences.