

Wojciech Konaszczuk\*

# Legislacyjne rozwiązania w zakresie przeciwdziałania cyberprzestępczości w prawie podatkowym – wybrane zagadnienia \*\*

## 1. WSTĘP

Problematyka cyberprzestępczych wyludzeń podatkowych należy do nowych, rozwijających się obszarów wyspecjalizowanej działalności przestępczej zarówno w Polsce, Unii Europejskiej, jak i poza jej granicami. Szczególnym utrudnieniem dla organów ochrony prawnej w tym zakresie jest konieczność łączenia wyspecjalizowanej wiedzy z zakresu nauk ścisłych obejmujących matematykę, informatykę, kryptografię, jak też nauk prawnych obejmujących specjalizacje w obrębie prawa podatkowego, karnego, administracyjnego oraz, co bardzo ważne, z zakresu prawa międzynarodowego. To właśnie wiedza z zakresu tej ostatniej dyscypliny warunkuje harmonizację interdyscyplinarnej wiedzy systemów prawa kontynentalnego i *common law*, tworząc ramy do podjęcia szerszej dyskusji na temat trendów zwalczania cyberprzestępczości podatkowej na świecie.

## 2. GENEZA CYBERPRZESTĘPCZOŚCI

W polskiej literaturze przedmiotu zarówno teoretycznej, jak i praktycznej zagadnienie genezy cyberprzestępczości jest analizowane w dosyć nikłym zakresie. Związane jest to niewątpliwie z faktem, że źródeł przestępczości komputerowej (dalej cyberprzestępczość) należy poszukiwać w miejscu powstania narzędzia, którym posługują się przestępcy oraz rozwoju technologii komputerowych w Stanach Zjednoczonych Ameryki. Do pojawienia się cyberprzestępczości wymagane było zaistnienie narzędzia, którym można posłużyć się do dokonania przestępstwa (komputera), oprogramowania, sieci oraz czynnika ludzkiego. Samo pojęcie „komputer” jest dość trudno definiowalne. W profesjonalnej literaturze przedmiotu uznaje się, że komputerem jest maszyna mogąca przetwarzać dowolne dane zgodnie z określonym algorytmem. Techniczna strona budowy takiej maszyny jest bez znaczenia. Taką definicję jako pierwszy zaprezentował Alan Matison Turing<sup>1</sup>,

\* Dr hab. Wojciech Konaszczuk jest profesorem Uniwersytetu Marii Curie-Skłodowskiej w Lublinie, Polska, ORCID: 0000-0003-0364-0727, e-mail: wojciech.konaszczuk@poczta.umcs.lublin.pl

\*\* Data zgłoszenia tekstu przez autora: 6.05.2021 r.; data przyjęcia tekstu przez redakcję do publikacji: 15.07.2021 r.

<sup>1</sup> A.M. Turing (1912–1954) brytyjski matematyk i kryptolog, konstruktor maszyny Turinga, uważany jest za twórcę informatyki. Uważany jest również za jednego z ojców i prekursorów sztucznej inteligencji. Zob. szerzej S. Homer, A.L. Selman, *Computability and Complexity Theory*, Berlin 2001, s. 35 i n.

znany jako twórca maszyny Turinga. Maszyna Turinga to nic innego jak urządzenie, na które zakładana jest taśma z polami, w której każde pole może być jednym z  $N$  stanów. W zależności od stanu maszyny, zmienia się jego stan i przesuwa w lewo lub prawo. Działanie to charakteryzuje tzw. zjawisko przetwarzania danych za pomocą instrukcji, czyli programu. Komputer jest zatem urządzeniem pozwalającym na przetwarzanie zakresu danych za pomocą narzędzia jakim jest program, czyli instrukcja. Założenie to jest spójne z pokrywającymi się w szerokim zakresie elementami definicji komputera. Z kolei według Georgesa Ifraha – historyka i matematyka, komputer „jest automatem, złożonym z urządzenia wejściowego i wyjściowego, pamięci, jednostki centralnej dokonującej wszelkiego rodzaju przekształceń danych wyrażonych w postaci ciągów znaków (stanowiących materialne przedstawienie zakodowanych informacji), który pozwala – w granicach fizycznych możliwości urządzenia – wykonywać wszelkie obliczenia typu symbolicznego (zatem rozwiązywać wszelkie zadania, których rozwiązanie można wyrazić w postaci algorytmu) pod kierunkiem jednostki sterującej działającej zgodnie z programem zapisanym w pamięci (i wobec tego traktujące instrukcje wykonawcze w ten sam sposób, co dane przeznaczone do przetworzenia)”<sup>2</sup>.

Kierując się elementami definicji komputera, należy wskazać, że urządzenie o takich parametrach została zaprojektowane przez Charlesa Babbage’a. Opracował on złożony i skomplikowany mechanizm składający się z układu wejścia–wyjścia, układu uruchamiania, magazynu, młynka, urządzenia drukującego służącego do przetwarzania danych liczbowych. Mechanizm był uruchamiany mechanicznie, zaś sterowanie odbywało się przy użyciu metalowych kart perforowanych. Perforowanie dawało możliwość wykonywania złożonych operacji interakcyjnych, a co za tym idzie podejmowania decyzji o wyborze programu w zależności od wyników cząstkowych.

Pod koniec XIX i na początku XX w. wielu uczonych i praktyków podejmowało próby budowy komputera, jak również kontynuowania dzieła Ch. Babbage’a, do największych zaś osiągnięć należy zaliczyć prace Percy Ludgate’a<sup>3</sup>, Torresa Quovendo<sup>4</sup>, Kondrada Zusa<sup>5</sup>.

Pierwszą maszyną analityczną, którą można zakwalifikować jako komputer, był produkt marki IBM znany pod nazwą IBM ASCC (*Automatic Sequence Controlled Calculators*), będący maszyną obliczeniową znaną pod nazwą Mark 1. Została ona zaprojektowana przez Howarda Hathaway Aikena<sup>6</sup>. Produkty IBM, znane pod nazwami Mark 1–4 zrewolucjonizowały i zmonopolizowały rozwój światowej informatyki na przestrzeni kolejnych dekad. Komputery nie miały jednak możliwości komunikowania się ze sobą. Jednym z punktów zwrotnych w historii informatyki był pomysł, aby komputery połączyć ze sobą w celu intensyfikacji ich mocy obliczeniowej.

<sup>2</sup> J. Dauben, G. Ifrah, “Book Review”: The Universal History of Numbers and The Universal History of Computing (part 1), styczeń 2002, s. 25.

<sup>3</sup> W 1840 r. ogłosił projekt maszyny analitycznej podobny do dzieła Ch. Babbage’a z modyfikacjami.

<sup>4</sup> W 1914 r. zaprezentował modyfikację dzieła Ch. Babbage’a, polegającą na wykorzystaniu podzespołów elektromagnetycznych w miejsce perforowanych płyt metalowych.

<sup>5</sup> W latach 1935–1939 zaprojektował szereg maszyn analitycznych, prekursorów dzisiejszych komputerów.

<sup>6</sup> H.H. Aiken (1900–1973) amerykański fizyk, matematyk. W 1939 r. uzyskał stopień doktora nauk na Uniwersytecie Harvarda. W 1947 r. stworzona przez niego maszyna znalazła zastosowanie w armii amerykańskiej, zaś pamięć komputera opierała się na dysku magnetycznym (zob. szerzej I.B. Cohen, *Howard Aiken: Portrait of a Computer Pioneer*, “MIT Press” 1999, s. 73–114).

W ten sposób powstała tzw. sieć komputerowa, umożliwiająca przesyłanie informacji między urządzeniami. Początki sięgają badań naukowych, które zostały zapoczątkowane na Uniwersytecie Kalifornijskim w Los Angeles. W dniu 29.09.1969 r. uruchomiono na tej uczelni pierwsze węzły sieci określanej jako ARPANET (*Advanced Research Project Agency Network*), wykorzystywane do badań na rzecz armii USA. Celem ARPANET-u było utworzenie sieci dającej możliwość komunikowania się pomiędzy komputerami bez ośrodka centralnego (serwera). Miało to gwarantować skuteczność i bezpieczeństwo wymiany informacji na wypadek wojny, nawet w przypadku uszkodzenia jej fragmentu. Dość istotną wadą założenia wiązała się z brakiem programu (protokołu) pozwalającego na obsługę sieci, dzięki któremu informacje mogły być przesyłane na odległość w sieciach rozproszonych. Na lata 1969–1971 przypadają intensywne prace na czołowych uczelniach amerykańskich, które miały umożliwić rozwiązanie problemu transferu informacji przez sieć i protokołu go obsługującego. Na przełomie lat 1971/1972 zaprezentowano dwa protokoły, a mianowicie TCP (*Transmission Control Protocol*) oraz IP (*Internet Protocol*). TCP jest protokołem pozwalającym na transmisję danych w postaci pakietów. Polega to na tym, że u nadawcy dane są rozbijane na pakiety, wysyłane przez sieć i następnie składane w jedną całość u odbiorcy. Z kolei IP jest protokołem związanym z adresowaniem. Protokół IP nie jest potrzebny w sytuacji, kiedy w sieci występują wyłącznie dwa komputery – nadawcy i odbiorcy. Problem pojawia się z chwilą, kiedy w sieci występują więcej niż dwie jednostki. Wówczas w braku protokołu IP pakiety danych TCP nie są w stanie dotrzeć do adresata. Służy temu właśnie protokół IP, który jest metodą adresowania komputerów w sieci. W czasie rozwoju sieć ARPANET stosowała pierwotnie wiele wersji związanych z identyfikacją komputerów. Do unifikacji doszło dopiero na początku lat 80. XX w. za sprawą Jonathana Bruce'a Postela<sup>7</sup>, który w latach 1982–1983 stworzył podstawy powiązania protokołu IP (adresowego) z hierarchicznie budowanymi nazwami domen internetowych – DNS (*Domain Name Servers*). DNS pozwala na przyporządkowanie adresów numerycznych do nazw literowych. Proces ten został uwieńczony przez przyjęcie w armii amerykańskiej protokołu TCP/IP oraz DNS jako standardów sieci. W tym samym czasie wszedł w życie termin internet, który po porzuceniu projektu ARPANET w 1989 r. stał się sferą rozwojową dla uczelni i organizacji naukowych.

O wykorzystaniu internetu dla celów komercyjnych, początkowo w Stanach Zjednoczonych, można mówić dopiero po roku 1991. W tym roku bowiem amerykańska *National Science Foundation* (NSF) zezwoliła na udostępnienie sieci szerszemu gronu użytkowników.

Warto również wspomnieć o rozwoju WWW czyli *World Wide Web* będącą obecnie najbardziej popularną formą wykorzystania internetu. W 1991 r. Tim Berners-Lee uznał za konieczne upowszechnienie wyników swoich badań poświęconych fizyce molekularnej. W tym celu stworzył podstawy kodu HTML (*Hyper Text Markup Language*) po to, aby w dwa lata później opracować projekt pierwszej w historii przeglądarki internetowej o nazwie Mosaic, która dała podstawę

<sup>7</sup> J.B. Postel (1943–1988) profesor informatyki, wykładowca Uniwersytetu Los Angeles (UCLA), twórca wielu innowacyjnych rozwiązań, w tym m.in. pierwszego protokołu elektronicznych wiadomości SMTP (*Simple Mail Transfer Protocol*).

do opracowania ulepszonej wersji przeglądarki o nazwie Netscape. Z punktu widzenia przedmiotowej analizy Netscape jako przeglądarka jest o tyle istotna, gdyż jako pierwsza dawała możliwość przesyłania danych bezpiecznym połączeniem szyfrowanym. Można było zatem przysyłać poufne dane, które były szyfrowane i mogły być odczytane wyłącznie przez ich adresata.

Powyżej opisane wynalazki dały bardzo silny impuls do rozwoju światowej sieci i internetu. Zanim zostanie określona siatka pojęciowa terminu „cyberprzestępczość”, należy zastanowić się nad momentem, od którego datuje się działanie określane tym mianem. Termin ten jest zbieżny z początkami wykorzystania sieci do przesyłania informacji, tj. w przybliżeniu z końcem lat 70. XX w. W 1983 r. Amerykanin Kevin Mitnick uzyskuje nieautoryzowany dostęp do sieci ARPANET, za co zostaje wobec niego orzeczona kara 6 miesięcy bezwzględnego pozbawienia wolności<sup>8</sup>. Jest to jeden z pierwszych przypadków popełnienia przestępstwa w zakresie cyberprzestępczości przy wykorzystaniu komputera, za który została orzeczona kara pozbawienia wolności.

### 3. ZARYS SIATKI POJĘCIOWEJ BADAŃ TEMATU

Na wstępie należy podkreślić, że podobnie jak pojęcie terroryzm, tak pojęcie cyberprzestępczość nie ma jednolitej definicji. Wydaje się słuszne wskazanie, na podstawie analizy literatury światowej, że pojęcie to dogłębnie zostało zbadane przez teoretyków i praktyków zajmujących się problematyką prawa karnego, zwłaszcza na gruncie prawa amerykańskiego<sup>9</sup>. Biorąc pod uwagę uniwersalizm pojęć badaczy amerykańskich, należy zaznaczyć, że na określenie tego pojęcia używa się takie terminy jak: cyberprzestępczość (*cyber crime*), przestępczość komputerowa (*computer crime*) czy w wreszcie przestępczość związana z komputerami (*computer related crime*). Uwzględniając szereg różnych definicji, należy przyjąć na gruncie prawa międzynarodowego, że cyberprzestępczość jest to każdy rodzaj działalności niezgodny z normami prawa wewnętrznego lub międzynarodowego, którego skutek przekracza granice państwa, zaś jej narzędzie lub też cel stanowi urządzenie w postaci komputera. Oczywiście taka definicja powinna być rozbudowana o uściślenie, że chodzi o naruszanie przez działanie oprogramowania, albowiem przedmiotem nie jest sam komputer jako urządzenie fizyczne, lecz zainstalowane oprogramowanie na tym komputerze służące określonemu celowi. W tym zakresie niewątpliwie istotne znaczenie mają inicjatywy podejmowane na forum międzynarodowym w postaci m.in. definicji przyjętej przez Organizację Narodów Zjednoczonych podczas X Kongresu Narodów Zjednoczonych w sprawie Zapobiegania Przestępczości i Traktowaniu Przestępców, który odbył się 11–17.04.2000 r. w Wiedniu<sup>10</sup>. Zgodnie z przyjętą definicją *sensu largo* są to wszystkie działania o nielegalnym charakterze popełniane za pomocą komputerów i odnoszące się do systemów lub

<sup>8</sup> B. Gengler, *Super-hacker Kevin Mitnick takes a plea*, DOI: 10.1016/S1361-3723(99)90141-0 (dostęp: 30.03.2021 r.).

<sup>9</sup> Tak też zauważa M. Siwicki w: *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo” 2012/7–8, s. 241–244.

<sup>10</sup> SOC/CP/214 6 of April 2000, <http://www.un.org/press/en/2000/20000406.soccp214.doc.html> (dostęp: 30.03.2021 r.).

sieci komputerowych. Z kolei w ujęciu *sensu stricto* pojęciem cyberprzestępczości objęto działania wymierzone przeciw bezpieczeństwu systemów komputerowych lub programów obsługujących bazy danych<sup>11</sup>.

Na podstawie wytycznych wiedeńskiego kongresu na forum Organizacji Narodów Zjednoczonych przyjęto Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej<sup>12</sup>. Jakkolwiek Konwencja, jako ratyfikowana umowa międzynarodowa wiąże wprost, to w cytowanym dokumencie ONZ nie wskazał na jednolite pojęcia cyberprzestępczości. Warto jednak pochylić się nad niektórymi regulacjami umowy, które w sposób bezpośredni odnoszą się do tego zjawiska na gruncie prawa międzynarodowego. W art. 2 lit. a cytowanej umowy wskazano, że „zorganizowana grupa przestępcza” oznacza posiadającą strukturę grupę składającą się z trzech lub więcej osób, istniejącą przez pewien czas oraz działającą w porozumieniu w celu popełnienia jednego lub więcej poważnych przestępstw określonych na podstawie niniejszej konwencji, dla uzyskania, w sposób bezpośredni lub pośredni, korzyści finansowej lub innej korzyści materialnej”. Z kolei lit. d charakteryzuje pojęcie „mienia” jako wszelkiego rodzaju dobra, zarówno materialne, jak i niematerialne, ruchome i nieruchome, a także dokumenty oraz instrumenty prawne stanowiące o istnieniu tytułu własności lub uprawnień do tych dóbr.

W art. 29 określono obowiązek szkolenia oraz pomocy technicznej, co odnosi się m.in. do cyberprzestępczości. Zgodnie z brzemieniem tego artykułu, każde państwo (również Polska) będące stroną umowy w niezbędnym zakresie będzie inicjowało, rozwijało i udoskonalało specjalne programy szkoleniowe dla organów ścigania, w tym prokuratorów, sędziów śledczych oraz pracowników służby celnej, jak również innych pracowników zajmujących się zapobieganiem, wykrywaniem oraz kontrolą przestępstw objętych zakresem niniejszej Konwencji. Takie programy mogą obejmować staże oraz wymiany personelu. Szkolenia powinny obejmować „metody wykorzystywane w zwalczaniu międzynarodowej przestępczości zorganizowanej popełnianej przy wykorzystaniu komputerów, sieci telekomunikacyjnych lub innych form nowoczesnych technologii<sup>13</sup>”, jak również zagadnienia z zakresu metod przesłuchania podejrzanych. Z tym ostatnim problemem stykamy się w kontekście problematyki ochrony praw procesowych podejrzanych (oskarżonych) i orzecznictwa Europejskiego Trybunału Praw Człowieka (dalej ETPC) z punktu widzenia instytucji przyznania się do winy<sup>14</sup>.

W odniesieniu do interesujących nas zagadnień, pojęciem cyberprzestępczości objęte będą wszelkie pozaprawne działania, które mają na celu wpłynięcie na sferę podlegającą szczególnej ochronie prawnej. W ogólnym zarysie działania te mają na celu przejęcie kontroli nad systemami operacyjnymi urządzeń komputerowych (w tym serwerów) w celu wpłynięcia na bieg zdarzeń po myśli sprawców, kiedy te działania są podjęte umyślnie.

<sup>11</sup> [https://digitallibrary.un.org/record/432663/files/A\\_CONF.187\\_15-EN.pdf](https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf) (dostęp: 30.03.2021 r.).

<sup>12</sup> United Nations Convention against Transnational Organized Crime (UNTOC) – Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych 15.11.2000 r. (Dz.U. z 2005 r. Nr 18, poz. 158) – dalej Konwencja.

<sup>13</sup> Art. 29 lit. h.

<sup>14</sup> Zasygnalizowania wymaga koncepcja tzw. doktryny Salduz, w której ETPC podnosił czynniki wpływające w sposób ujemny na poziom wartości dowodu z przyznania się oskarżonego, który złożył je w okolicznościach wpływających na oświadczenie woli. Zob. szerzej na ten temat E. Kruk, *Kilka uwag na temat przyznania się do winy w trybie art. 335 k.p.k.*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego” 2019/105, s. 86–89.

W chwili obecnej, oprócz wspomnianej Konwencji Narodów Zjednoczonych, brak jest jednolitych regulacji o charakterze powszechnym odnoszących się do zapobiegania zagrożeniom związanym z cyberprzestępczością<sup>15</sup>.

Obok aktów obowiązujących, należy zwrócić uwagę na wytyczne rezolucji Zgromadzenia Ogólnego ONZ z 17.03.2010 r. w sprawie globalnej kultury cyberbezpieczeństwa i ochrony krytycznych infrastruktur informacyjnych<sup>16</sup>. Szczegółowy postulat zawarty jest w art. 13 cytowanej rezolucji. Zgodnie z jego brzmieniem wzywa się władze państw członkowskich do przeglądu oraz nowelizacji przepisów prawnych dotyczących cyberprzestępstw, prywatności, danych osobowych, prawa handlowego, podpisów cyfrowych kryptografii, wykorzystywania w tym celu regionalnych i międzynarodowych instrumentów, i standardów prawnych<sup>17</sup>.

Z kolei w obrębie Unii Europejskiej pojęciem *cybercrime* posługuje się w praktyce Komisja Europejska (KE), formułując tezę, że cyberprzestępczością są „działania przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom”<sup>18</sup>. Została ona uzupełniona w dyrektywie 2002/58/WE, która zawiera zobowiązanie państw członkowskich do zapewnienia odpowiedniego poziomu praw i wolności, w szczególności praw związanych z wykorzystaniem komunikacji elektronicznej<sup>19</sup>.

Problematyka ochrony przetwarzania danych osobowych i ochrony prywatności w kontekście prawa dowodowego i karalności pojawiła się także na gruncie polskiej nauki. Koncepcja wykorzystania narzędzi matematycznych w służbie polskiego procesu karnego pojawiła się w nowatorskiej koncepcji Adama Tarachy. Wykorzystanie algorytmu matematycznego w zastosowaniu cyfrowym umożliwia bowiem identyfikację nie tylko pojazdu, ale także twarzy. W chwili obecnej w praktyce organów ścigania służb na całym świecie narzędzie algorytmów wykorzystywane jest do identyfikacji jednostek roboczych (komputerów). Dzieje się to najczęściej

<sup>15</sup> Spośród organizacji o charakterze regionalnym zajmujących się problematyką zwalczania cyberprzestępczości niewątpliwie należy wymienić Radę Europy. W listopadzie 2001 r. Rada Europy przyjęła Konwencję o cyberprzestępczości, która stanowi jedno z ważniejszych osiągnięć przed zagrożeniami w sieci. Konwencja oprócz tego, że zdefiniowała pojęcia przestępstw przeciwko poufności i dostępności danych informatycznych oraz systemów, to zobowiązała sygnatariuszy do przyjęcia środków o charakterze prawnym mającym na celu zabezpieczenie danych informatycznych przed ingerencją w nie, utratą lub modyfikacją (Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie 23.11.2001 r., Dz.U. z 2015 r. poz. 728). W odniesieniu do działalności Unii Europejskiej w przedmiotowym zakresie należy wspomnieć o dyrektywie 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotyczącej przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej. Dyrektywa zawiera zobowiązanie państw członkowskich do zapewnienia odpowiedniego poziomu praw i wolności w szczególności praw związanych z wykorzystaniem komunikacji elektronicznej (Dz.Urz. WE L 201 z 2002 r., s. 37 ze zm.) – dalej dyrektywa 2002/58/WE, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32002L0058&from=PL> (dostęp: 30.03.2021 r.).

<sup>16</sup> Rezolucja została przyjęta 21.12.2009 r., zaś dzień 17.03.2010 r. jest datą publikacji oficjalnego dokumentu ONZ, [http://www.un.org/en/ga/search/view\\_doc.asp?symbol=A/RES/64/211](http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211) (dostęp: 30.03.2021 r.) – dalej rezolucja.

<sup>17</sup> *“Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime”.*

<sup>18</sup> Jednolity tekst Komunikatu Komisji do Parlamentu Europejskiego oraz Komitetu Regionów, Bruksela 22.07.2007 r., <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52007DC0267&from=PL> (dostęp: 30.03.2021 r.).

<sup>19</sup> <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32002L0058&from=PL> (dostęp: 30.03.2021 r.).



w sytuacjach, kiedy mamy do czynienia z tzw. trasowaniem cebulowym, z którego dość często korzystają przestępcy w celu zatarcia śladów numeru IP komputera. Nie ma problemu do chwili, kiedy karta sieciowa komputera lub IP (personalny numer identyfikacyjny) nie są przypisane do tożsamości osoby fizycznej. Wątpliwości co do możliwości naruszenia ochrony danych osobowych pojawiają się w sytuacji, kiedy jednostka robocza na skutek wprowadzenia zmian konfiguracyjnych posiada powiązanie z tożsamością osoby, którą można zidentyfikować w oparciu o imię, nazwisko lub co najważniejsze – wspomniany IP. Sytuacja ta może być analogiczna do opisanej przez A. Tarachę w odniesieniu do algorytmu rozpoznawania twarzy<sup>20</sup>.

Biorąc pod uwagę szereg różnorodnych rozwiązań na poziomie ponadnarodowym (powszechnym i regionalnym), szczególnie istotna w omawianym zakresie pozostaje zatem współpraca państw o charakterze wielostronnym. Jej istotnym elementem jest określenie dziedzin, które podlegają zagrożeniom. Przede wszystkim należy tu wymienić dwa podstawowe rodzaje danych, które wiążą się z funkcjonowaniem sieci, a mianowicie: dane niestrukturalne i dane strukturalne. Pierwsza grupa obejmuje wszelkiego rodzaju skany dokumentów, umów, rozwiązań, które występują w wersji fizycznej oraz cyfrowej, stanowiące w odniesieniu do całości ok. 80% wszystkich danych. Druga grupa z kolei obejmuje dane strukturalne, które mogą występować oraz funkcjonować jedynie w formie cyfrowej. Dane te, które stanowią 20% całości, stanowią podstawę wykorzystywaną przez specjalistyczne oprogramowanie używane przez urzędy na świecie<sup>21</sup>.

#### 4. CHARAKTERYSTYKA PRZESTĘPCZOŚCI PODATKOWEJ NA GRUNCIE MIĘDZYNARODOWYM I UE

Przystąpienie Polski do Unii Europejskiej dało nie tylko asumpt do promowania swobody przepływu kapitału, towarów i usług, lecz także przyczyniło się do poszerzenia prowadzenia działalności polegającej na wyludzeniach podatkowych na szerszą skalę. W tym sensie, zanim przedstawione zostaną przykłady i specyfika wyludzeń podatkowych, należy wskazać na prawne formy ochrony obrotu podatkowego przyjętego w UE. Do jednego z podstawowych dokumentów unijnych w przedmiocie regulowania podatków pośrednich, tj. VAT-u, należy dyrektywa Rady Unii Europejskiej 2006/112/WE z 28.11.2006 r. w sprawie wspólnego systemu podatku od wartości dodanej<sup>22</sup>. Regulacja została wydana na podstawie dyspozycji zawartej w art. 93 Traktatu ustanawiającego Wspólnotę Europejską<sup>23</sup> po uwzględnieniu wniosku Komisji Europejskiej, jak również opinii Parlamentu Europejskiego. Ważne, że w art. 1 dyrektywy VAT wprowadzono jednolitą definicję podatku VAT oraz uregulowano zasady odnoszące się do jego stosowania.

<sup>20</sup> Zob. szerzej A. Taracha, *Wykorzystanie algorytmów w postępowaniu karnym – wybrane zagadnienia*, „Studia Iuridica Lublinensia” 2020/5, t. XXIX, s. 301 i n.

<sup>21</sup> L. Haines, D. Lyle, *The Digital Oil field Today*, „Oil and Gas Investor” 2004 (suplement), s. 5–6.

<sup>22</sup> Dz.Urz. WE L 347 z 2006 r., s. 1 ze zm. – dalej dyrektywa VAT. Słuszne wydaje się podkreślenie, że od chwili wejścia w życie rozwiązań normatywnych w niej zaproponowanych do dnia dostępu do bazy danych Dziennika Urzędowego Unii Europejskiej (z 28.03.2021 r.) doszło do 106 zmian opublikowanych w postaci zmian, upoważnień zarówno w odniesieniu do państw członkowskich UE, terytoriów tych państw, stanów nadzwyczajnych wywołanych przez pandemię SARS-COV-2, czy Wielkiej Brytanii w związku z jej wystąpieniem z Unii.

<sup>23</sup> Wersja skonsolidowana Dz.Urz. UE C 325 z 2006 r., s. 37 – dalej TWE.

W związku z tym dyrektywą objęto wszystkie podatki VAT w państwach członkowskich. Zasada wspólnego systemu VAT polega na zastosowaniu do towarów i usług ogólnego podatku konsumpcyjnego dokładnie proporcjonalnego do ceny towarów i usług, niezależnie od liczby transakcji, które mają miejsce w procesie produkcji i dystrybucji poprzedzającym etap obciążenia tym podatkiem. VAT, obliczony od ceny towaru lub usługi według stawki, która ma zastosowanie do takiego towaru lub usługi, jest wymagalny od każdej transakcji, po odjęciu kwoty podatku poniesionego bezpośrednio w różnych składnikach kosztów. Wspólny system VAT stosuje się aż do etapu sprzedaży detalicznej włącznie. Co ważne, wprowadzono katalog opodatkowanych czynności (art. 2 dyrektywy VAT). Zgodnie z tym katalogiem na terytorium UE opodatkowaniu podlegają następujące transakcje: odpłatna dostawa towarów na terytorium państwa członkowskiego przez podatnika działającego w takim charakterze; odpłatne wewnątrzwspólnotowe nabycie towarów na terytorium państwa członkowskiego dokonywane: przez podatnika działającego w takim charakterze lub przez osobę prawną niebędącą podatnikiem, gdy sprzedawcą jest podatnik działający w takim charakterze, który nie korzysta ze zwolnienia dla małych przedsiębiorstw przewidzianego w art. 282–292 dyrektywy VAT i który nie jest objęty przepisami art. 33 i 36; w przypadku nowych środków transportu przez podatnika lub osobę prawną niebędącą podatnikiem, w przypadku których inne nabycia nie podlegają opodatkowaniu VAT zgodnie z art. 3 ust. 1, lub przez jakąkolwiek inną osobę niebędącą podatnikiem; w przypadku wyrobów podlegających akcyzie, jeżeli od wewnątrzwspólnotowego nabycia naliczany jest podatek akcyzowy na terytorium państwa członkowskiego zgodnie z dyrektywą 92/12/EWG<sup>24</sup> przez podatnika lub osobę prawną niebędącą podatnikiem, w przypadku których inne nabycia nie podlegają opodatkowaniu VAT zgodnie z art. 3 ust. 1; odpłatne świadczenie usług na terytorium państwa członkowskiego przez podatnika działającego w takim charakterze; import towarów.

Z kolei w treści art. 4 dyrektywy VAT znalazły się wyłączenia z opodatkowania, i co charakterystyczne, z praktyki wynika, że nie stanowią one obecnie przedmiotu przestępczego procederu wyłudzeń podatkowych VAT przez sprawców. Do najważniejszych wyłączeń należy zaliczyć: wewnątrzwspólnotowe nabycia towarów używanych, dzieł sztuki, przedmiotów kolekcjonerskich lub antyków, określonych w art. 311 ust. 1 pkt 1–4, jeżeli sprzedawca jest podatnikiem-pośrednikiem działającym w takim charakterze, a nabyte towary zostały opodatkowane VAT w państwie członkowskim rozpoczęcia wysyłki lub transportu towarów zgodnie z procedurą marży przewidzianą w art. 312–325 oraz wewnątrzwspólnotowe nabycia używanych środków transportu określonych w art. 327 ust. 3, jeżeli sprzedawca jest podatnikiem-pośrednikiem działającym w takim charakterze, a nabyty używany środek transportu został opodatkowany VAT w państwie członkowskim rozpoczęcia wysyłki lub transportu, zgodnie z procedurą przejściową mającą zastosowanie do używanych środków transportu. Z kolei do przedmiotowych wyłączeń określonych w art. 312–325 odnosi się szczególna procedura przewidziana dla podatników pośredników. W odniesieniu do nich wprowadzono definicję „ceny sprzedaży”

<sup>24</sup> Dyrektywa Rady 92/12/EWG z 25.02.1992 r. w sprawie ogólnych warunków dotyczących wyrobów objętych podatkiem akcyzowym, ich przechowywania, przepływu oraz kontrolowania (Dz.Urz. EWG L 76 z 23.03.1992 r., s. 1 ze zm.).



i „ceny nabycia” (art. 312 dyrektywy VAT). Zgodnie z nimi „cena sprzedaży” oznacza wszystkie składniki wynagrodzenia uzyskanego lub do uzyskania przez podatnika pośrednika od nabywcy lub osoby trzeciej, włączając w to subwencje bezpośrednio związane z transakcją, podatki, cła, opłaty i należności oraz koszty dodatkowe takie jak: prowizja, koszty opakowania, transportu i ubezpieczenia, którymi podatnik-pośrednik obciąża nabywcę. Z kolei „cena nabycia” oznacza wszystkie składniki wynagrodzenia, uzyskanego lub do uzyskania przez dostawcę od podatnika-pośrednika.

Jak się okazuje, znajomość sfery objętej przedmiotowym podatkiem była i wciąż jest istotna z punktu widzenia pragmatyki przestępczej działalności.

Zasadnicze bowiem znaczenie dla prowadzenia wyłudzeń podatkowych na szeroką skalę ma unormowanie, z którego wynika, że w UE przyjęto (podobnie jak w Polsce) rozwiązanie polegające na tym, iż podatek ma charakter pośredni, co zwiększa wartość towaru na każdym etapie sprzedaży. Jest on uiszczany przy każdej transakcji w ciągu: producent, pośrednik, sprzedawca, konsument. Ponadto jest on neutralny dla podatników w łańcuchu za wyjątkiem odbiorcy końcowego, który ponosi w pełni jego ciężar. Jest to bowiem konsekwencją faktu przierzucalności podatku oraz możliwości stosowania systemowych odliczeń. Co za tym idzie, wprowadzono w Unii mechanizm odliczeń na każdym etapie zmiany właściciela towaru, tj. na każdym etapie obrotu towaru.

Unijne dyrektywy przesądziły o tym, że VAT jest jednym z nielicznych podatków w UE o zharmonizowanym charakterze i jednolitej strukturze. Oznacza to, że docelowo wszystkie państwa członkowskie mają być objęte jednolitym opodatkowaniem w zakresie podatku od wartości dodanej. W związku z tym, istotna część rodzimej ustawy o podatku od towarów i usług<sup>25</sup> stanowi implementację do polskiego systemu prawnego norm unijnych, wyrażonych w poszczególnych dyrektywach dotyczących VAT.

Jednym z kluczowych rozwiązań w obrocie podlegającym opodatkowaniu jest fakt, że wewnątrzspółnotowa dostawa towarów jest opodatkowana stawką zerową VAT. Na podkreślenie zasługuje wyjaśnienie terytorialnego zakresu obowiązywania dyrektywy. Pojęcie „wewnątrzspółnotowy” odnosi się do „Wspólnoty” i „terytorium Wspólnoty” (art. 5 dyrektywy VAT). Oznacza ono terytorium każdego państwa członkowskiego Wspólnoty, do którego ma zastosowanie TWE zgodnie z jego art. 299, z wyłączeniem niektórych terytoriów wymienionych w art. 6 dyrektywy VAT. Wyłączeniu podlegają m.in. następujące terytoria: Athos, Wyspy Kanaryjskie, francuskie departamenty zamorskie, Wyspy Alandzkie, Wyspy Normandzkie<sup>26</sup>.

Z punktu widzenia przestępczej działalności w Polsce i w UE kluczowym elementem jest dyspozycja art. 42 ust. 1 wspomnianej ustawy o VAT. Zgodnie z jego brzmieniem „Wewnątrzspółnotowa dostawa towarów podlega opodatkowaniu według stawki podatku 0%, pod warunkiem że: 1) podatnik dokonał dostawy na rzecz nabywcy posiadającego właściwy i ważny numer identyfikacyjny dla

<sup>25</sup> Ustawa z 11.03.2004 r. o podatku od towarów i usług (tekst jedn.: Dz U. z 2021 r. poz. 685) – dalej ustawa o VAT.

<sup>26</sup> Polska ustawa o VAT zawiera szczegółowe określenie terytoriów, które na mocy umów międzynarodowych zostały wyłączone spod właściwości terytorialnej UE. Wyłączeniu podlegają m.in.: wyspa Helgoland i terytorium Buessingen z RFN; Ceuta, Melilla, Wyspy Kanaryjskie z Królestwa Hiszpanii, Livigno, Campione d'Italia, część jeziora Lugano z Republiki Włoskiej, Góra Athos z Republiki Greckiej.

transakcji wewnątrzspółnotowych, nadany przez państwo członkowskie właściwe dla nabywcy, zawierający dwuliterowy kod stosowany dla podatku od wartości dodane, który nabywca podał podatnikowi; 2) podatnik przed upływem terminu do złożenia deklaracji podatkowej za dany okres rozliczeniowy, posiada w swojej dokumentacji dowody, że towary będące przedmiotem wewnątrzspółnotowej dostawy zostały wywiezione z terytorium kraju i dostarczone do nabywcy na terytorium państwa członkowskiego inne niż terytorium kraju; 3) podatnik składając deklarację podatkową, w której wykazuje tę dostawę towarów, jest zarejestrowany jako podatnik VAT UE”. Opodatkowanie zerową stawką VAT posiada bardzo istotne znaczenie dla działalności przestępczej. W przeciwieństwie do zwolnień podatkowych, obrót towarami opodatkowanymi na poziomie stawki zerowej daje podstawę do odliczeń naliczonego wcześniej podatku VAT.

Oszustwo zwane karuzelą podatkową można określić jako sposób wyłudzenia zwrotu podatku VAT przez podmioty, które nie są do tego uprawnione, występujące w ciągu pozornych lub faktycznych transakcji obrotu objętego opodatkowaniem (w którym musi wystąpić opodatkowanie zerową stawką VAT), w których, w ramach wcześniej zaplanowanych przez sprawców, uczestniczą świadome lub nieświadome podmioty gospodarcze. Na podstawie dostępnej literatury, statystyk oraz przekazów medialnych można przypuszczać, że genezy „przestępstw karuzelowych” można poszukiwać we Włoszech i Hiszpanii już w początkach XXI w., co związane było z działalnością zorganizowanych grup przestępczych w tych państwach.

Podobne, czy wręcz identyczne rozwiązania przyjęte przez polskiego ustawodawcę obowiązują na terenie wszystkich państw członkowskich. Dało to podstawę rozwoju wyłudzeń podatkowych podejmowanych na terytoriach wszystkich państw członkowskich w ramach działalności określanej jako „przestępstwa karuzelowe”. W procesie karuzeli podatkowej, bez względu na liczbę podmiotów gospodarczych uczestniczących na terytorium UE w obrocie, zawsze musi wystąpić płatnik podatku, który nie dokonuje jego zapłaty, określanej jako „*missing trader*”, czyli „znikający handlarz”. Następne podmioty, które w nim uczestniczą, to „słupy” i „znikający handlarze”. Już w początkowych etapach rozwoju tego typu przestępczej działalności we Włoszech i w Hiszpanii do tej funkcji wykorzystywano osoby fizyczne o niskim statusie materialnym (bezdomni, żebracy), na które były rejestrowane podmioty gospodarcze. W procederze uczestniczą także „bufory” będące podmiotami, w których osoby zarządzające mają świadomość prowadzenia przestępczej działalności. Zadaniem tych podmiotów jest odprowadzanie należności do instytucji skarbowych. Z kolei rolą „brokera” jest sprzedaż towaru zagranicznemu podmiotowi ze stawką zerową VAT. Broker dokonuje również odliczenia wcześniej zapłaconego podatku. Rolą „brokera” jest również uzyskanie zwrotu podatku od organów państwa (który zresztą wcześniej nie został zapłacony przez „znikającego handlarza”). W początkowej fazie rozwoju przestępczości wyłudzeń VAT „brokerami” były podmioty będące sprawcami. W późniejszym okresie w rolach „brokerów” zaczęły występować tzw. słupy.

Cały schemat można przedstawić w sposób następujący: podatnik A (z siedzibą poza granicami Polski, lecz w którymś z państw członkowskich UE) sprzedaje podatnikowi B (z siedzibą w Polsce) towar w ramach wewnątrzspółnotowej dostawy towarów. Stawka VAT to 0%, więc nie płaci on podatku. Podatnik B sprzedaje

towar dalej podatnikowi C już w ramach wewnątrzkrajowej dostawy towarów. Dla uproszczenia przyjmijmy, że cena netto towaru to 100, a stawka VAT to 10%. W związku z tym, podatnik B składa deklarację VAT, w której podatek naliczony to 0, a podatek należny to 10. Tego ostatniego nie płaci jednak, a następnie, zgodnie ze swoją rolą, znika. Podatnik C sprzedaje towar podatnikowi D za 200. Podatek naliczony to 10, podatek należny to 20. Podatnik C wpłaca więc do Urzędu Skarbowego 10. Następnie D sprzedaje towar A w ramach wewnątrzwspólnotowej dostawy towarów. Stawka VAT w tym przypadku to 0%, podatek należny więc to 0, a podmiot D występuje o zwrot podatku naliczonego, tj. 20<sup>27</sup>.

## 5. POLSKA SPECYFIKA PODATKOWA A WYŁUDZENIA PODATKOWE

Polski katalog przestępstw o charakterze podatkowym uregulowany jest w głównej mierze w Kodeksie karnym skarbowym<sup>28</sup>, jak również w ustawach regulujących konkretne podatki. Przestępstwa podatkowe, a także wykroczenia skarbowe zasadniczo uregulowane są w rozdziale 6 k.k.s. W grę wchodzi także unormowania części szczególnej Kodeksu karnego<sup>29</sup>.

W przypadku naruszeń regulacji z zakresu prawa podatkowego ważne jest określenie dwóch zasadniczych atrybutów związanych z przestępstwem, a mianowicie sposobu, czy też metody polegającej na naruszeniu oraz dobra prawnie chronionego. Pierwszy atrybut został powyżej wyjaśniony. Polega on na wykorzystywaniu w ramach działalności cyberprzestępczej komputerów i sieci do przesyłania informacji. Drugi element wymaga krótkiej analizy.

Najogólniej należnością podatkową są publicznoprawne, nieodpłatne, przymusowe oraz bezwrotne świadczenia pieniężne na rzecz państwa. Podatki stanowią główne źródło dochodów państwa oraz umożliwiają finansowanie jego działalności. Każdy, kto znajduje się w sytuacji objętej podatkiem, ma obowiązek go zapłacić.

Z punktu widzenia naruszeń przepisów prawa podatkowego najczęściej do naruszania norm prawnych dochodzi w odniesieniu do podatku od towarów i usług oraz podatku akcyzowego. Wprowadzenie w 1993 r. podatku od towarów i usług oraz podatku akcyzowego<sup>30</sup> stworzyło nową możliwość dokonywania przestępstw polegających na wyłudzeniu nienależnych kwot od Skarbu Państwa. W szczególności taka możliwość zyskała na popularności pojedynczych sprawców, jak również grup przestępczych po akcesji Polski do Unii Europejskiej w 2004 r. W szczególności aktywnej działalności przestępczej poddany jest podatek VAT. Wynika to z jego specyfiki, a mianowicie z tego, że jest to z założenia należność, która obciąża finalnego odbiorcę towaru lub usługi. W przypadku prowadzenia działalności gospodarczej, podmiot ma prawo do potrącenia podatku naliczonego od wartości podatku należnego. Zobowiązanie podatkowe jest zatem różnicą pomiędzy kwotą podatku należnego z tytułu prowadzonego obrotu handlowego przez podmiot

<sup>27</sup> Zob. szerzej na ten temat T. Oczkowski, *Problematyka karnoprawnej oceny wyłudzenia podatku VAT*, „Prokuratura i Prawo” 2009/7–8, s. 82–87.

<sup>28</sup> Ustawa z 10.09.1999 r. – Kodeks karny skarbowy (tekst jedn.: Dz.U. z 2021 r. poz. 53) – dalej k.k.s.

<sup>29</sup> Ustawa z 6.06.1997 r. – Kodeks karny (tekst jedn.: Dz.U. z 2020 r. poz. 1444) – dalej k.k.

<sup>30</sup> Ustawa z 8.01.1993 r. o podatku od towarów i usług oraz o podatku akcyzowym (Dz.U. z 1993 r. Nr 11, poz. 50 ze zm.).

a kwotą podatku zapłaconego, który jest związany z nabyciem towarów lub usług niezbędnych do uzyskania obrotu. Zobowiązanie po stronie podmiotu powstaje wtedy, gdy wartość podatku należnego jest większa od podatku naliczonego w danym okresie rozliczeniowym. Zobowiązanie nie powstaje, jeśli kwota podatku należnego jest niższa lub równa wartości podatku naliczonego. Z punktu widzenia zagrożeń związanych z uszczupleniami podatkowymi niebezpieczeństwo naruszeń powstaje w sytuacji, kiedy podatek naliczony jest wyższy od podatku należnego. Podatnikom przysługuje wówczas prawo do wystąpienia do organu podatkowego o bezpośredni zwrot podatku naliczonego, przewyższającego wartość podatku należnego. Takie uprawnienie przysługuje podmiotom prowadzącym działalność, którzy mają prawo do odliczenia naliczonego podatku od towarów lub usług. Ustalenie wysokości zobowiązania podatkowego, tj. zapłaty lub zwrotu podatku VAT, odbywa się w oparciu na dokumencie deklaracji podatkowej. Uprawnienie to z kolei powstaje na podstawie uzyskanych dokumentów, tj. faktur VAT, które są wystawiane przez podatników tego podatku. W tym sensie mogą występować oszustwa charakterystyczne dla wszystkich podatków, których większość odnosi się do uszczupień podatkowych. Zasadniczo terminem „uszczuplenie podatkowe” określa się bezprawne działanie polegające na nienależnym obniżeniu obciążeń podatkowych. Zarówno w doktrynie, jak i praktyce ugruntowane jest stanowisko, że obowiązek podatkowy jest elementem różnicującym typ przestępstwa oszustwa klasycznego od oszustwa skarbowego. Pierwszy typ chroni mienie przed zamachami, które nie są związane z jednoczesnym naruszeniem dobra w postaci obowiązku podatkowego, drugi natomiast chroni mienie przed zamachami, które realizowane są z bezprawnym wykorzystaniem regulacji z zakresu prawa podatkowego<sup>31</sup>. Problematyka „uszczupień podatkowych” stanowiła także przedmiot orzecznictwa sądowego. W wyroku z 19.03.2008 r., II KK 347/07<sup>32</sup>, Sąd Najwyższy (dalej SN), powołując się na brzmienie ówczesnej ustawy o podatku od towarów i usług z 11.03.2004 r.<sup>33</sup>, wywiódł wniosek, że fakt wystawienia „wadliwej” faktury VAT w pierwszej kolejności rodzi obowiązek podatkowy, zaś w drugiej zawsze narusza przepis art. 62 § 2 k.k.s. Jak konkluduje Sąd, można żywić wątpliwości co do trafności poglądu, że czynności sprawcy, które sprowadzają się do działania fingującego istnienie obowiązku podatkowego wyłącznie w celu osiągnięcia korzyści kosztem Skarbu Państwa za pomocą fikcyjnych dokumentów dla przeprowadzenia realnej czynności, stanowią jedynie przestępstwo określone w przepisach Kodeksu karnego, nie zaś przestępstwo skarbowe. Sąd stanął na stanowisku, że podstawą kwalifikacji prawnej wszystkich tego rodzaju przestępstw powinien być art. 76 § 1 k.k.s.

Z kolei w orzeczeniu z 12.08.2008 r., V KK 76/08<sup>34</sup>, SN stwierdził, że: „Porównanie treści art. 76 § 1 k.k.s. i art. 286 § 1 k.k. prowadzi do oczywistego wniosku, że pierwszy z nich jest przepisem *lex specialis* w stosunku do drugiego. Znamiona przestępstwa z art. 76 § 1 k.k.s. mieszczą się całkowicie w ogólniej ujętym opisie działania sprawcy przestępstwa z art. 286 § 1 k.k., typizując szczególny rodzaj

<sup>31</sup> P. Kardas, *O wzajemnych relacjach między przepisem art. 76 § 1 k.k.s. a przepisem art. 286 § 1 k.k.*, „Prokuratura i Prawo” 2008/12, s. 24 i n.

<sup>32</sup> LEX nr 388503.

<sup>33</sup> Dz.U. z 2020 r. poz. 106 ze zm.

<sup>34</sup> LEX nr 449041.

oszustwa prowadzącego do wyłudzenia nienależnego zwrotu podatkowej należności publicznonprawnej. Aktualnie wystawca faktury niemającej w ogóle odzwierciedlenia w stanie faktycznym, ma także obowiązek uiszczenia podatku VAT. Zatem przepisem, który należy zastosować przy kwalifikacji prawnej czynu polegającego na wyłudzeniu nienależnego zwrotu podatku VAT, jest art. 76 § 1 k.k.s.”

Zbliżony pogląd przyjął wrocławski Sąd Apelacyjny (dalej SA), który w orzeczeniu z 3.09.2009 r., II AKA 105/09<sup>35</sup>, stwierdził, że: „[j]eżeli wystawca «fikcyjnej» faktury VAT, niedokumentującej rzeczywistego zdarzenia gospodarczego lub osoba posługująca się taką fakturą, wykorzystuje ją do naliczania należnego podatku VAT, a także określenia innego obowiązku podatkowego (np. podatku dochodowego przez pomniejszenie dochodu), to osoby te godzą w obowiązki podatkowe i odpowiadają za przestępstwo skarbowe z art. 62 § 2 k.k.s. W wypadku, gdy sprawca zmierza do wyłudzenia nienależnego zwrotu podatku VAT, to popełnia przestępstwo skarbowe z art. 62 § 2 k.k.s. Jednak w wypadku, gdy «fikcyjną» fakturę wystawiono wyłącznie dla przestępczych celów pozapodatkowych, np. dla wyłudzenia kredytu lub dotacji dla siebie lub innej osoby albo dla doprowadzenia innej osoby do niekorzystnego rozporządzenia mieniem przez fingowanie dobrej kondycji gospodarczej i wiarygodności kontrahenta umowy, to wystawca takiej faktury lub osoba posługująca się nią powinny nadal odpowiadać na podstawie przepisów ustawy karnej innej niż k.k.s. (np. z art. 297 k.k. lub z art. 286 § 1 k.k.)”. W ten sposób można przyjąć tezę, że kwalifikacja prawna zachowań sprawców o ich tożsamym charakterze zależeć będzie od tego, w co sprawcy godzą. Jeśli godzą w obowiązki podatkowe, wówczas odpowiadają za przestępstwa natury skarbowej. Takie twierdzenie byłoby zasadniczo słuszne, gdyby nie problematyka związana z mieniem. Należy zdawać sobie bowiem sprawę z tego, że w rzeczywistości zamiar sprawców ukierunkowany jest zasadniczo na mienie należące do Skarbu Państwa. To właśnie mienie stanowi przedmiot zamachu w przypadku popełniania czynów związanych z wystawianiem „fikcyjnych” faktur VAT. Ochrona mienia Skarbu Państwa stanowić powinna zasadniczy przedmiot ochrony prawnej. Warto pochylić się tu nad Ordynacją podatkową, z której należy wywodzić, że „obowiązkiem podatkowym jest wynikająca z ustaw podatkowych nieskonkretyzowana powinność przymusowego świadczenia pieniężnego w związku z zaistnieniem zdarzenia określonego w tych ustawach”<sup>36</sup>. Ustawa o podatku od towarów i usług precyzuje w art. 19a, że: „Obowiązek podatkowy powstaje z chwilą dokonania dostawy towarów lub wykonania usługi.(...) W odniesieniu do przyjmowanych częściowo usług, usługę uznaje się również za wykonaną, w przypadku wykonania części usługi, dla której to części określono zapłatę”.

Przechodząc do podsumowania rozważań dotyczących dobra chronionego w kontekście judykatury i doktryny, należy wysunąć tezę, że ustawodawca pochylił się nad koncepcją uznającą, iż uszczuplenia podatkowe w kontekście stosowania ustawy o podatku od towarów i usług dotyczą bezpośrednio mienia należącego do Skarbu Państwa.

Skala negatywnych zjawisk związana z wyłudzeniami podatku VAT wpłynęła na kształt nowelizacji Kodeksu karnego w tym zakresie. Od 2017 r.

<sup>35</sup> LEX nr 519593.

<sup>36</sup> Art. 4 ustawy z 29.08.1997 r. – Ordynacja podatkowa (Dz.U. z 2020 r. poz. 1325 ze zm.).

w związku ze zmianami k.k. i k.k.s. zwiększyła się znacząco odpowiedzialność sprawców za naruszenia w zakresie wykonania ustawy o podatku od towarów i usług. Przede wszystkim doprecyzowane zostało pojęcie faktury. Zgodnie z art. 115 § 14a k.k. fakturą jest dokument, o którym mowa w art. 2 pkt 31 ustawy o VAT<sup>37</sup>.

Jednocześnie określono sankcje za wystawienie faktury poświadczającej nieprawdę. Zgodnie z art. 271a § 1 k.k. osoba poświadczając nieprawdę co do okoliczności faktycznych mogących mieć znaczenie dla określenia wysokości należności publicznoprawnej lub jej zwrotu albo zwrotu innej należności o charakterze podatkowym lub takiej faktury lub faktur używa, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Zgodnie z § 2 tegoż artykułu, jeżeli sprawca dopuszcza się czynu określonego w § 1 wobec faktury lub faktur, zawierających kwotę należności ogółem, której wartość lub łączna wartość jest większa niż pięciokrotność kwoty określającej mienie wielkiej wartości albo z popełnienia przestępstwa uczynił sobie stałe źródło dochodu, podlega karze pozbawienia wolności na czas nie krótszy od lat 3.

Należy podkreślić, że ustawodawca odniósł się także do podrobienia lub przerobienia faktury w celu użycia za autentyczną. Zgodnie bowiem z treścią art. 270a § 1 podrobienie lub przerobienie faktury w zakresie okoliczności faktycznych mogących mieć znaczenie dla określenia wysokości należności publicznoprawnej lub jej zwrotu albo zwrotu innej należności o charakterze podatkowym lub takiej faktury jako autentycznej używa, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Natomiast – według § 2 – jeżeli sprawca dopuszcza się czynu określonego § 1 wobec faktury lub faktur, zawierających kwotę należności ogółem, której wartość lub łączna wartość jest większa niż pięciokrotność kwoty określającej mienie wielkiej wartości albo z popełnienia przestępstwa uczynił sobie stałe źródło dochodu, podlega karze pozbawienia wolności na czas nie krótszy od lat 3.

Teza o przedmiocie ochrony mienia Skarbu Państwa jako dobra prawnie chronionego, pojawiająca się dość często w doktrynie, została ugruntowana w art. 277a § 1 k.k. Zgodnie bowiem z treścią tego artykułu osoba dopuszczająca się przestępstwa przerobienia, podrobienia faktury, poświadczenia nieprawdy co do okoliczności faktycznych mających mieć wpływ na wysokość daniny publicznoprawnej zawierających kwotę należności ogółem, której wartość lub łączna wartość jest większa niż dziesięciokrotność kwoty określającej mienie wielkiej wartości, podlega karze pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności.

W przestępstwach polegających na uszczupleniach z tytułu VAT stosuje się metodę polegającą na uzyskaniu kwoty ze sprzedaży towarów, od których w rzeczywistości nie zapłacono podatku. Ustalenie momentu powstania obowiązku podatkowego pozwala wyznaczyć przedmiot ochrony, i w konsekwencji wnioskować o zamiarze sprawców omawianych przestępstw. Ważne jest również to, że sprawcy uszczupleń podatkowych w przypadku zarówno podatku VAT, jak i podatku akcyzowego działają z zamiarem bezpośrednim ukierunkowanym na wyrządzenie szkody w mieniu Skarbu Państwa. Wypełnia to zatem znamiona klasycznego przestępstwa oszustwa.

<sup>37</sup> Zgodnie z cytowanym art. 2 pkt 31 fakturą jest „dokument w formie papierowej lub w formie elektronicznej zawierający dane wymagane ustawą i przepisami wydanymi na jej podstawie”.



Celem sprawców nie jest bowiem unikanie płacenia podatków, lecz osiągnięcie korzyści majątkowych pochodzących od Skarbu Państwa. Chodzi tu o „przejęcie” środków przez sprawców przestępstw poprzez wystawienie fikcyjnych faktur.

Metodologia postępowania sprawców może być różnorodna. W zależności od specjalizacji grupy, może ona przybierać postać działań w zakresie usług lub działalności w zakresie towarów. Jeżeli chodzi natomiast o metody wykorzystywane przez grupy lub pojedynczych sprawców, to albo polegają one na wystawianiu fikcyjnych faktur między podmiotami, albo na zawieraniu rzeczywistych umów, w których dochodzi do niczym nieuzasadnionego wzrostu wartości sprzedaży towaru lub usługi w celu naliczenia wyższego podatku VAT. Najczęstszym przypadkiem wykorzystywanym w uszczupleniach podatkowych jest niewątpliwie pozorowanie zdarzeń gospodarczych, które w rzeczywistości nie wystąpiły lub istotne zwiększenie wartości dokonywanych obrotów towarami lub usługami.

Przechodząc do omówienia przykładów związanych ze znacznymi uszczupleniami podatkowymi w Polsce, należy niewątpliwie odnieść się do kilku dziedzin szczególnie narażanych na przestępczy proceder ze względu na wysokie obroty, popularność towarów oraz możliwość szybkiego i znacznego uszczuplenia Skarbu Państwa. Do takich obszarów należą następujące dziedziny: obrót stalą, obrót węglem, obrót paliwami, obrót elektroniką oraz urządzeniami HI-TECH, w tym komputerami oraz telefonami komórkowymi. Zjawisko uszczuplenia dochodów podatkowych nie należy do nowych. Ważne od jakiego momentu rozpoczął się proces sukcesywnego procesu uszczupień podatkowych na istotną skalę. Jednym z pierwszych potwierdzonych działań na dużą skalę był wewnątrzspółnotowy obrót stalą. W 2010 r. według oficjalnych danych wszystkie państwa członkowskie UE sprzedały do Polski wyroby stalowe o łącznej wadze 374 000 ton metrycznych. Z kolei według polskich raportów waga sprowadzonych do Polski wyrobów stalowych wyniosła 149 000 ton metrycznych. Różnica z dokumentacji wyniosła 225 000 ton metrycznych wyrobów stalowych, na które nie było faktycznego pokrycia. Sytuacja ta była możliwa z kilku powodów. Po pierwsze, lata 2010–2012 to gwałtowny rozwój infrastruktury drogowej, budowano wówczas węzły komunikacyjne, drogi szybkiego ruchu, stadiony w związku z przygotowaniem do EURO 2012. Po drugie, formułowanie nowych zamówień wiązało się z koniecznością wykorzystania środków unijnych. Po trzecie, intensyfikacji uległa wymiana towarowo-usługowa w obrębie Unii z ukierunkowaniem na Polskę. Koniunktura gospodarcza została wykorzystana przez ugrupowania mające na celu uszczuplenie majątku Skarbu Państwa. Według danych Prokuratury Generalnej, w latach 2006–2012, Skarb Państwa stracił na mechanizmach karuzelowych od 1 do 18 miliardów złotych. Przy podaniu tych danych należy jednak zaznaczyć, że dotyczą one wyłącznie spraw, które wpłynęły do prokuratury, mogą więc być to dane zaniżone. Do 2016 r. brak było oficjalnych szacunków Ministerstwa Finansów, jednak próbują dokonać ich eksperci, według których luka podatkowa w Polsce (w zakresie podatku VAT) może wynosić nawet od 5 do 67 miliardów złotych<sup>38</sup>. Zakładając, że jedynie czwarta część tej kwoty byłaby wydrenowana z budżetu

<sup>38</sup> <http://podatki.onet.pl/konferencja-w-bcc-polska-traci-miliardy-z-powodu-1,19925,5297532,agencyjne-detel> (dostęp: 30.03.2021 r.).

za pomocą mechanizmów karuzelowych, i tak daje to sumę znaczącą. Dogłębne zbadanie struktury i skali oszustw podatkowych w Polsce nie było przedmiotem zainteresowania resortu finansów, który nigdy nie przeprowadził w tym zakresie własnych analiz. Tymczasem według szacunków Eurostatu, różnica między eksportem do Polski raportowanym przez kraje unijne a ewidencjonowanym w Polsce importem towarów istnieje wciąż powiększająca się luka. Dynamikę bezprawnych uszczupień dochodów Skarbu Państwa z tytułu podatku VAT przedstawiła w raporcie z 31.03.2014 r. Najwyższa Izba Kontroli (NIK).

Dość istotny i zasadniczy problem wpływający na wysokość wyłudzeń podatkowych do „dużej nowelizacji ustawy w 2017 roku” wiązał się z nierównoprawnym traktowaniem niektórych towarów podlegających opodatkowaniu. Ustawa o VAT w art. 105a wprowadziła pojęcie „solidarnej odpowiedzialności”. Zgodnie z brzmieniem tego artykułu: „1. Podatnik, o którym mowa w art. 15, na rzecz którego dokonano dostawy towarów, o których mowa w załączniku nr 13 do ustawy, odpowiada solidarnie wraz z podmiotem dokonującym tej dostawy za jego zaległości podatkowe w części podatku proporcjonalnie przypadającej na dostawę dokonaną na rzecz tego podatnika, jeżeli:

- 1) wartość towarów, o których mowa w załączniku nr 13 do ustawy, nabywanych od jednego podmiotu dokonującego ich dostawy, bez kwoty podatku przekroczyła w danym miesiącu kwotę 50 000 zł, oraz
- 2) w momencie dokonania dostawy towarów, o których mowa w załączniku nr 13 do ustawy, podatnik wiedział lub miał uzasadnione podstawy do tego, aby przypuszczać, że cała kwota podatku przypadająca na dokonaną na jego rzecz dostawę tych towarów lub jej część nie zostanie wpłacona na rachunek urzędu skarbowego.

2. Podatnik miał uzasadnione podstawy do tego, aby przypuszczać, że cała kwota podatku przypadająca na dokonaną na jego rzecz dostawę towarów lub jej część nie zostanie wpłacona na rachunek urzędu skarbowego, jeżeli okoliczności towarzyszące tej dostawie towarów lub warunki, na jakich została ona dokonana, odbiegały od okoliczności lub warunków zwykle występujących w obrocie tymi towarami, w szczególności jeżeli cena za dostarczone podatnikowi towary była bez uzasadnienia ekonomicznego niższa od ich wartości rynkowej”.

Przed nowelizacją zatem nabywcy paliw płynnych na stacji benzynowej w przypadku, kiedy obrót był przedmiotem przestępczej działalności, ponosili solidarną odpowiedzialność. Paradoks tej regulacji polegał na tym, że sfera obrotu paliwami płynnymi przed końcem 2015 r. należała do najbardziej zagrożonych i takich, w których dochodziło do najwiękzych wyłudzeń podatkowych.

## **6. PROBLEMATYKA CYBERPRZESTĘPCZOŚCI A WYŁUDZENIA PODATKOWE**

Przechodząc do zagadnień związanych z problematyką związków cyberprzestępczości i wyłudzeń podatkowych, należy przedstawić kilka ważnych sformułowań, które determinują analizę i rozważania na gruncie prawa wewnętrznego i ponadnarodowego (unijnego). W pierwszej kolejności należy podkreślić, że sprawcza działalność w zakresie cyberprzestępczych wyłudzeń podatkowych nie byłaby możliwa bez

sprawnego funkcjonowania światowego systemu bankowego. Po drugie, wyłudzenia podatkowe w tym zakresie mają charakter interdyscyplinarny. Nie ma obecnie możliwości podzielenia sfery przestępczej działalności na sferę wewnętrzną czy ponadnarodową. Sprawę komplikuje fakt, że systemy sieciowe nie posiadają granic, stąd cyberprzestępczość podatkowa ma charakter uniwersalny. Po trzecie, obowiązujące ujednolicone przepisy podatkowe w Unii Europejskiej nie odzwierciedlają kar grozących za przestępce wyłudzenia. Sfera ta jest niejednolita, sprawiająca istotne trudności organom ścigania państw należących do UE. Po czwarte, bardzo duży odsetek popełnianych wyłudzeń cyberprzestępczych wiąże się z działalnością podmiotów operujących poza Unią, należy tu wymienić: Ukrainę, Federację Rosyjską, Białoruś, Chiny itd. Co się z tym wiąże, utrudnia to dodatkowo zapobieganie i zwalczanie tego rodzaju przestępczości.

Niewątpliwym zagrożeniem w tym zakresie jest liberalizacja sektora bankowego w ramach UE. Restrykcyjne zasady przepływu kapitału ustalone w Traktacie ustanawiającym Europejską Wspólnotę Gospodarczą (Rzym, 1957 r.)<sup>39</sup> przez kilka dekad podlegały znacznemu stępieniu i liberalizacji. W 1960 i 1962 r. zostały wprowadzone dyrektywy powodujące liberalizację w zakresie inwestycji bezpośrednich, krótko- i średnioterminowych kredytów handlowych i związanych z nimi poręczeń i gwarancji, a także transferów prywatnych związanych z przemieszczaniem się osób. Z kolei 17.11.1986 r. wprowadzono regulację w dużym stopniu znoszącą ograniczenia „w zakresie niezbędnym do funkcjonowania wspólnego rynku”. Odnosiła się ona do współpracy pomiędzy państwami członkowskimi a trzecimi i dotyczyła zasad zwrotu podatku od wartości dodanej podatnikom nieposiadającym siedziby na terytorium Wspólnoty (obecnie Unii). W zakresie przedmiotowej działalności ta zmiana przepisów miała przełomowe znaczenie. Jeszcze większe znaczenie miała dyrektywa Rady Wspólnot Europejskich z czerwca 1988 r. Zakładała ona pełną liberalizację, a co za tym idzie, zobowiązywała do usunięcia wszelkich ograniczeń w przepływie kapitału. Chodziło o to, by obywatele państw członkowskich uzyskali swobodny dostęp do systemów finansowych partnerów, tj. inwestycji, pożyczek. Nadała ona bardzo duże znaczenie transakcjom krótkoterminowym, dzięki czemu obywatele państw Wspólnoty mogli bez żadnych ograniczeń zakładać konta bankowe w innych państwach członkowskich, a także mieli pełną swobodę w zaciąganiu pożyczek. Do pełnej liberalizacji doszło 1.07.1990 r. Ustanowiono wtedy pełną swobodę przepływu kapitału i ten dzień określa się jako początek pierwszego etapu Unii Gospodarczej i Walutowej.

Wartość nadrzędną w tym zakresie mają postanowienia rozdziału 4 Traktatu o funkcjonowaniu Unii Europejskiej<sup>40</sup>, odnoszącego się do kapitału i płatności. Artykuł 63 wprowadza zakaz wszelkich ograniczeń w przepływie kapitału między państwami członkowskimi oraz między państwami członkowskimi a państwami trzecimi. Również zakazane są ograniczenia we wszelkich płatnościach między państwami członkowskimi oraz między państwami członkowskimi a państwami trzecimi. Istotnym elementem sprzyjającym cyberprzestępczym wyłudzeniom

<sup>39</sup> [http://oide.sejm.gov.pl/oide/index.php?option=com\\_content&view=article&id=14436&Itemid=436](http://oide.sejm.gov.pl/oide/index.php?option=com_content&view=article&id=14436&Itemid=436) (dostęp: 30.03.2021 r.).

<sup>40</sup> Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 47 – dalej TFUE.

podatkowym są postanowienia art. 65 TFUE<sup>41</sup>. Zgodnie bowiem z jego brzmieniem państwa członkowskie są upoważnione do: a) stosowania odpowiednich przepisów ich prawa podatkowego traktujących odmiennie podatników ze względu na różne miejsce zamieszkania lub inwestowania kapitału; b) podejmowania wszelkich środków niezbędnych do zapobiegania naruszeniom ich ustaw i aktów wykonawczych, zwłaszcza w sferze podatkowej i w dziedzinie nadzoru ostrożnościowego nad instytucjami finansowymi lub ustanowienia procedur deklarowania przepływu kapitału do celów informacji administracyjnej bądź statystycznej lub podejmowania środków uzasadnionych powodami związanymi z porządkiem publicznym lub bezpieczeństwem publicznym.

Państwa, co wcześniej wskazano, mają możliwość swobodnego regulowania kwestii podatkowych, zwłaszcza w zakresie odpowiedzialności za wyłudzenia.

Jak nadmieniono, bardzo istotnym elementem są regulacje z zakresu prawa bankowego oraz instrumenty finansowe. W przypadku problematyki cyberprzestępczych wyłudzeń podatkowych istotne są regulacje ustawy z 29.08.1997 r. – Prawo bankowe<sup>42</sup> oraz ustawy z 29.07.2005 r. o obrocie instrumentami finansowymi<sup>43</sup>.

Ustawa – Prawo bankowe w znowelizowanej w 2017 r. postaci jest w pełni dostosowana do wymogów unijnego prawa bankowego. Przede wszystkim zostały uwzględnione regulacje skierowane w stronę ułatwień w obrocie finansowym, wynikające z: rozporządzenia Parlamentu Europejskiego i Rady (UE) 575/2013 z 26.06.2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniającego rozporządzenie 648/2012/UE<sup>44</sup>; rozporządzenia Parlamentu Europejskiego i Rady (UE) 596/2014 z 16.04.2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady, i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE<sup>45</sup> oraz rozporządzenia delegowanego Komisji 2017/565/UE z 25.04.2016 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy<sup>46</sup>. Artykuł 5 ust. 4 pr. bank. nałożył na podmioty (podatników) prowadzących działalność gospodarczą obligatoryjny obowiązek wykonywania czynności bankowych wyłącznie przez banki. Z kolei według art. 5 ust. 1 pr. bank. czynnościami bankowymi są: 1) przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów; 2) prowadzenie innych rachunków bankowych;

<sup>41</sup> Dodany przez art. G lit. D pkt 15 Traktatu o Unii Europejskiej (wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 13) w związku z przystąpieniem Polski do Unii Europejskiej;

– zmieniony i według numeracji ustalonej przez art. 12 ust. 1 i 2 Traktatu z Amsterdamu zmieniającego Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie i niektóre związane z nimi akty (Dz.U. z 2004 r. Nr 90, poz. 864 ze zm.) w związku z przystąpieniem Polski do Unii Europejskiej;

– zmieniony i według numeracji ustalonej przez art. 2 pkt 2 lit. b pkt 61 oraz art. 5 ust. 1 i 2 Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz.Urz. UE C 306 z 2007 r., s. 1) z dniem 1.12.2009 r. (sporządzony w Lizbonie 13.12.2007 r.) (Dz.U. z 2009 r. Nr 203, poz. 1569 ze zm.).

<sup>42</sup> Tekst jedn.: Dz.U. z 2020 r. poz. 1896 – dalej pr. bank.

<sup>43</sup> Tekst jedn.: Dz.U. z 2021 r. poz. 328 – dalej u.o.i.f.

<sup>44</sup> Dz.Urz. UE L 176 z 2013 r., s. 1 ze zm.

<sup>45</sup> Dz.Urz. UE L 173 z 2014 r., s. 1 ze zm.

<sup>46</sup> Dz.Urz. UE L 87 z 2017 r., s. 1 ze zm.

3) udzielanie kredytów; 4) udzielanie i potwierdzanie gwarancji bankowych oraz otwieranie i potwierdzanie akredytyw; 5) emitowanie bankowych papierów wartościowych; 6) przeprowadzanie bankowych rozliczeń pieniężnych; 7) wykonywanie innych czynności przewidzianych wyłącznie dla banku w odrębnych ustawach.

Jednocześnie uregulowano zagadnienia formy czynności prawnych. Oświadczenia woli związane z dokonywaniem czynności bankowych mogą być składane w postaci elektronicznej. Dokumenty związane z czynnościami bankowymi mogą być sporządzane na informatycznych nośnikach danych, jeżeli dokumenty te będą w sposób należyty utworzone, utrwalone, przekazane, przechowywane i zabezpieczone. Usługi związane z zabezpieczeniem tych dokumentów mogą być wykonywane przez banki, spółki tworzone przez banki wraz z innymi podmiotami, a także przedsiębiorstwa pomocniczych usług bankowych. Jeżeli ustawa zastrzega dla czynności prawnej formę pisemną, to uznaje się, że czynność dokonana w formie elektronicznej spełnia wymagania formy pisemnej, także wtedy gdy forma została zastrzeżona pod rygorem nieważności. Oświadczenia woli związane z dokonywaniem tych czynności mogą być składane w postaci elektronicznej.

Z dniem 1.07.2018 r. weszła w życie nowelizacja Prawa bankowego<sup>47</sup>, która uregulowała problematykę płatności VAT w drodze rachunku bankowego, w myśl tzw. płatności podzielonej – *split payment*. Wprowadzone zostało subkonto do rachunku rozliczeniowego prowadzonego przez bank<sup>48</sup> pozwalające na dokonywanie przelewów należnego podatku VAT. Dla rachunków rozliczeniowych prowadzonych dla tego samego posiadacza bank prowadzi jeden rachunek VAT, niezależnie od liczby prowadzonych dla tego posiadacza rachunków rozliczeniowych. W przypadku prowadzenia więcej niż jednego rachunku rozliczeniowego dla tego samego posiadacza, bank prowadzi, na wniosek tego posiadacza, więcej niż jeden rachunek VAT. W przypadku rachunków rozliczeniowych prowadzonych przez Narodowy Bank Polski dla tego samego posiadacza bank ten prowadzi rachunek VAT dla każdego rachunku rozliczeniowego. Narodowy Bank Polski prowadzi rachunek VAT dla więcej niż jednego rachunku rozliczeniowego tego samego posiadacza na jego wniosek lub na podstawie przepisów o finansach publicznych. Rachunek prowadzi się w walucie polskiej. Otwarcie i prowadzenie rachunku VAT nie wymaga zawarcia odrębnej umowy, jak również otwarcie i prowadzenie rachunku VAT jest wolne od dodatkowych prowizji i opłat dla banku. Środki pieniężne zgromadzone na rachunku VAT mogą być, zgodnie z ustaleniami stron, oprocentowane. Bank nie wydaje do rachunku VAT instrumentu płatniczego, albowiem jest on przyporządkowany do rachunku głównego. Rachunek VAT może być uznany wyłącznie środkami pieniężnymi pochodzącymi z tytułu zapłaty kwoty odpowiadającej kwocie podatku od towarów i usług, przy użyciu komunikatu przelewu, o którym mowa w art. 108a ust. 3 ustawy o VAT (dalej komunikat przelewu) oraz wpłaty kwoty podatku od towarów i usług przez podatnika, o którym mowa w art. 103 ust. 5a ustawy o VAT, na rzecz płatnika, o którym mowa w art. 17a tej ustawy przy użyciu komunikatu przelewu. Uznanie i obciążenie rachunku VAT jest dokonywane

<sup>47</sup> Ustawa z 15.12.2017 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw (Dz.U. z 2018 r. poz. 62 ze zm.).

<sup>48</sup> Rozdział 3a dodany przez art. 3 pkt 3 ustawy z 15.12.2017 r. Zob. przypis 47.

odpowiednio przez obciążenie albo uznanie rachunku rozliczeniowego posiadacza rachunku VAT prowadzonego w tym samym banku.

Do tego należy także wskazać na konieczność uwzględnienia przepisów wspomnianej ustawy o obrocie instrumentami finansowymi. Reguluje ona w sposób drobiazgowy możliwość korzystania z sieci informatycznych, wykorzystujących szyfrowane protokoły SSL (Secure Sockets Layer) do korzystania z rachunków bankowych oraz dokonywania płatności.

Należy też nadmienić, że ustawa wprowadziła zharmonizowaną z regulacjami UE definicję bezpośredniego dostępu elektronicznego<sup>49</sup>. Zgodnie z nią przez bezpośredni dostęp elektroniczny rozumie się, z uwzględnieniem art. 20 rozporządzenia 2017/565/UE, udostępnianie systemu obrotu instrumentami finansowymi własnego połączenia z tym systemem, umożliwiającego składanie zleceń mających za przedmiot instrumenty finansowe za pośrednictwem systemu teleinformatycznego członka lub uczestnika albo bez wykorzystywania takiego systemu.

Kluczowym zagadnieniem dla możliwości dokonywania trudnych do wykrycia wyłudzeń podatkowych w przestępstwach, głównie karuzelowych, jest rozwiązanie polegające na wystawianiu i przysyłaniu faktur w drodze elektronicznej. Do końca 2013 r. zasady wystawiania i przysyłania faktur w formie elektronicznej były regulowane rozporządzeniem z 28.03.2011 r. w sprawie faktur<sup>50</sup> oraz rozporządzeniem Ministra Finansów z 20.12.2012 r. w sprawie przysyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej<sup>51</sup>. Od 2014 r. wynikają one z przepisów ustawy o podatku od towarów i usług, do której z dniem 1.01.2014 r. zostały wprowadzone definicje faktury i faktury elektronicznej (art. 2 pkt 31 i 32 ustawy o VAT).

Definicja faktury jest odzwierciedleniem definicji faktury elektronicznej przyjętej w art. 217 dyrektywy 2006/112/WE. Faktura elektroniczna, tak samo jak faktura papierowa, musi zawierać wszystkie elementy wymagane przepisami o VAT. Dla uznania faktury za elektroniczną niezbędne jest, by pozostawała ona w dowolnym formacie elektronicznym w momencie zarówno jej wystawienia, jak i otrzymania. Jak wynika z uzasadnienia do zmian wprowadzonych ustawą z dniem 1.01.2014 r., faktury utworzone w formacie elektronicznym poprzez, przykładowo, programy księgowo lub edytory tekstu, które zostały wysłane lub otrzymane na papierze, choć będą fakturami w rozumieniu przepisów ustawy o VAT, nie będą uznane za faktury elektroniczne w rozumieniu zaproponowanej w pkt 32 definicji. Z drugiej strony, faktury sporządzone w formie papierowej, które zostały zeskanowane, wysłane i otrzymane w formie e-mail, mogą zostać uznane za faktury elektroniczne – pod warunkiem że wersja papierowa nie została wprowadzona do obrotu.

Zgodnie bowiem z art. 2 pkt 31 i 32 ustawy o VAT przez fakturę rozumie się dokument w formie papierowej lub w formie elektronicznej zawierający dane wymagane ustawą i przepisami wydanymi na jej podstawie. Jeżeli chodzi o fakturę

<sup>49</sup> Art. 3 pkt 2d u.o.i.f.

<sup>50</sup> Rozporządzenie Ministra Finansów z 28.03.2011 r. w sprawie zwrotu podatku niektórym podatnikom, wystawiania faktur, sposobu ich przechowywania oraz listy towarów i usług, do których nie mają zastosowania zwolnienia od podatku od towarów i usług (Dz.U. Nr 68, poz. 360 ze zm.).

<sup>51</sup> Dz.U. z 2012 r. poz. 1528.



elektroniczną, to rozumie się przez to fakturę w formie elektronicznej wystawioną i otrzymaną w dowolnym formacie elektronicznym.

Takie rozwiązanie legislacyjne jest rozwiązaniem po prostu korzystnym. Pozwala ona na obrót towarami i usługami faktycznie bez kontaktu fizycznego pomiędzy kontrahentami. Tworzy to sytuację dość skomplikowaną w przypadku ewentualnych postępowań przeciwko sprawcom wyłudzeń. W bardzo dużym stopniu komplikuje także sam proces poszukiwania sprawców, zwłaszcza w związku z faktem, że operacje bankowe mogą być dokonywane na różnych kontach poza granicami Polski oraz w różnych państwach.

## 7. PODSUMOWANIE I WNIOSKI KOŃCOWE

Obecnie, co należy jednoznacznie podkreślić, w przypadku cyberprzestępczych wyłudzeń podatkowych nie ma skutecznego sposobu na pełne przeciwdziałanie temu rodzajowi przestępczości. Dotychczasowe regulacje prawne oraz działania okazały się niewystarczające i nie pozwalają na skuteczne zabezpieczenie interesów Skarbu Państwa. Wiąże się to z faktem, że regulacje praw UE, jak również prawa wewnętrzne są niewystarczające wobec procedury wyłudzeń. Oszustwa, jak wynika z raportów kontrolnych NIK z lat 2011–2015, wykrywane były z dużym opóźnieniem, kiedy sprawcy już zdążyli zatrzeć większość śladów przestępczej działalności. Trudności występowały zarówno z ustaleniem, jak i odzyskaniem uszczuplonych kwot VAT. W przypadku Polski rozmiar luki podatku od towarów i usług utrzymywał się na poziomie wyższym niż średnia wielkość tego zjawiska w krajach unijnych. Według Komisji Europejskiej w latach 2010–2014 wzrosła ona z 18% do 31% możliwych do osiągnięcia dochodów VAT. Ta luka podatkowa, utrzymująca się w bardzo dużych rozmiarach, świadczy o nieefektywności polskiego systemu podatkowego i potrzebie wprowadzania nowych rozwiązań mających na celu ograniczenie oszustw podatkowych. Zgodnie z szacunkami KE zakłada się, że na terytorium całej UE odsetek cyberprzestępczych wyłudzeń podatkowych wynosi ok. 89% i z roku na rok jest coraz większy. Związane jest to z naturalną digitalizacją sfer działalności gospodarczej w Europie i na świecie. W związku z tym do najważniejszych rozwiązań należy ustawodawcza implementacja następujących koncepcji: a) ustanowienie centralnej bazy faktur VAT do ich wystawiania w ramach serwerów Ministerstwa Finansów w ramach Krajowego Rejestru Faktur (KRF), b) utworzenie europejskiej, publicznej bazy rachunków podatników VAT, zharmonizowanej z systemem operacyjnym Schengen, c) wprowadzenie obligatoryjnego w całej UE mechanizmu *split payment*, d) ograniczenie płatności gotówkowych na rzecz transferów bankowych, e) wprowadzenie ograniczeń w przypadkach udzielania pełnomocnictw do reprezentacji podatników wyłącznie do obywateli państwa, gdzie doszło do rejestracji podmiotu, f) wprowadzenie instytucji sygnalisty w prawie podatkowym z określonym honorarium.

Potrzebne są nowe środki usprawniające pobór i egzekucję podatków, zmiany w organizacji służb do zwalczania najpoważniejszych oszustw podatkowych, jak i zmiany na płaszczyźnie regulacji karnych w kierunku zapewnienia realnej możliwości karania sprawców oszustw podatkowych. Należy zatem rozważyć wyodrębnienie pionu lub służby wyspecjalizowanej do zwalczania oszustw podatkowych na wielką skalę, z wykorzystaniem fikcyjnych faktur, służby wyposażonej w procedury kontroli i uprawnienia adekwatne do wagi popełnianych przez zorganizowane grupy przestępstw.

### Summary

#### Wojciech Konaszczuk, *Legislative Solutions to Counteract Cybercrime in Tax Law. Selected Issues*

*The development of new technologies, in particular programming tools and the world wide web, has initiated a number of adverse phenomena, also in legal systems of various countries, Poland being one of them. The coronavirus-induced pandemic is an additional factor that intensified life moving to the network. This article analyses the fragmentary topic of tax law violations with the use of both hardware and software and countermeasures taken and legal solutions introduced in the sphere of international, EU and national laws. The conclusions of this paper set out guidelines aimed at limiting the use of the Internet as the platform for committing tax law violations or cybercrime.*

**Keywords:** *tax cybercrime, tax fraud, cross-border crime, taxpayer surveillance mechanisms, prevention of international crime*

### Streszczenie

#### Wojciech Konaszczuk, *Legislacyjne rozwiązania w zakresie przeciwdziałania cyberprzestępczości w prawie podatkowym – wybrane zagadnienia*

*Rozwój nowych technologii, w szczególności narzędzi programistycznych i światowej sieci internetu, powoduje pojawienie się wielu negatywnych zjawisk, także w systemach prawnych państw, w tym Polski. Dodatkowym argumentem intensyfikującym przeniesienie różnych dziedzin życia do sieci jest panująca pandemia koronawirusa. Przedmiotowy artykuł analizuje wycinek naruszeń prawa podatkowego przy wykorzystaniu urządzeń (hardware) i oprogramowania (software) oraz podjętych kontradziałani i wprowadzenia rozwiązań prawnych w sferze prawa międzynarodowego, unijnego i krajowego. W podsumowaniu wskazane są wytyczne, które w konsekwencji mają ograniczyć wykorzystanie medium internetu do popełniania naruszeń i cyberprzestępczości w prawie podatkowym.*

**Słowa kluczowe:** *cyberprzestępczość podatkowa, wyludzenia podatku, przestępczość transgraniczna, mechanizmy nadzoru nad podatnikami, zapobieganie przestępstwom o charakterze międzynarodowym*

### Literatura:

1. Cohen I.B., *Howard Aiken: Portrait of a Computer Pioneer*, MIT Press 1999.
2. Dauben J., Ifrah G., "Book Review": *The Universal History of Numbers and The Universal History of Computing* (part 1), styczeń 2002.
3. Haines L., Lyle D., *The Digital Oil field Today*, Oil and Gas Investor 2004 (suplement).
4. Homer S., Selman A.L., *Computability and Complexity Theory*, Berlin 2001.
5. Gengler B., *Super-hacker Kevin Mitnick takes a plea*, DOI: 10.1016/S1361-3723(99)90141-0
6. Kardas P., *O wzajemnych relacjach między przepisem art. 76 § 1 k.k.s. a przepisem art. 286 § 1 k.k.*, Prokuratura i Prawo 2008, nr 12.
7. Kruk E., *Kilka uwag na temat przyznania się do winy w trybie art. 335 k.p.k.*, Zeszyty Naukowe Uniwersytetu Rzeszowskiego 2019, nr 105.
8. Oczkowski T., *Problematyka karnoprawnej oceny wyludzenia podatku VAT*, Prokuratura i Prawo 2009, nr 7-8.
9. Siwicki M., *Podział i definicja cyberprzestępstw*, Prokuratura i Prawo 2012, nr 7-8.
10. Taracha A., *Wykorzystanie algorytmów w postępowaniu karnym – wybrane zagadnienia*, *Studia Iuridica Lublinensia* 2020, t. XXIX, nr 5.