ACTA IURIDICA RESOVIENSIA Nr 2(45)/2024
ISSN 2720-0574 DOI: 10.15584/actaires.2024.2.11

Filip Wyszyński

Uniwersytet w Białymstoku
ORCID: 0000-0002-0792-5730

ZDATNOŚĆ REGULACJI PRAWNOKARNYCH DO KOMPLEKSOWEJ OCHRONY PALIWOWEJ INFRASTRUKTURY KRYTYCZNEJ PRZED CYBERPRZESTĘPCZOŚCIĄ

Wprowadzenie

Przedmiotem analizy jest problematyka cyberprzestępczości[1] z punktu widzenia sektorów gospodarczych, które uznać można za wrażliwe („krytyczne") – tu: sektora paliwowego. Hipotezą główną jest założenie, że ochrona infrastruktury paliw jest w ujęciu prawnokarnym urzeczywistniana wyłącznie przez pryzmat ogólnego katalogu przestępstw. Wobec tego należy zweryfikować zdatność regulacji prawnokarnych do kompleksowej ochrony infrastruktury krytycznej przed cyberprzestępczością na tle infrastruktury paliwowej (cel badawczy). Innymi słowy, należy poddać ocenie to, czy obowiązujące regulacje prawnokarne we właściwy sposób chronią infrastrukturę krytyczną przed cyberprzestępstwami skierowanymi przeciwko bezpieczeństwu i integralności infrastruktury krytycznej. Poprzez pojęcie *krytyczność* (*infrastruktura krytyczna*) rozumieć należy te obszary działalności, które są identyfikowane jako kluczowe dla funkcjonowania państwa. W niniejszym opracowaniu rozważone zostaną prawnokarne aspekty ochrony infrastruktury krytycznej przed zagrożeniami związanymi z cyberprzestępczością na przykładzie infrastruktury paliwowej (ropy naftowej).

[1] Jako przestępstwa internetowe można klasyfikować takiego rodzaju czyny, przy których internet daje możliwość bądź ułatwia sprawcy popełnienie przestępstwa; tym samym przestępczość internetowa jest takim rodzajem przestępczości, gdzie bez użycia sieci nie mogłoby dojść do wypełnienia znamion określonego czynu zabronionego bądź sytuacja taka byłaby znacznie trudniejsza do zaistnienia. Zob. B. Hołyst, *Kryminologia*, Warszawa 2016, s. 315. Przestępczość z wykorzystaniem internetu przybiera różne formy, lecz jest szczególnie niebezpieczna, gdy obiektem cyberataku staje się podmiot sektora krytycznego, gdyż zagrożona jest niemal nieograniczona liczba osób oraz funkcjonowanie państwa i gospodarki. Zob. J. Sadowski, *Cybernetyczny wymiar współczesnych zagrożeń*, „Studia nad Bezpieczeństwem" 2017, nr 2, s. 64

Dodatkowo zastrzec należy, że analizie poddane zostaną przepisy Kodeksu karnego[2] jako podstawowej regulacji prawnokarnej (*sensu stricto*). Wskazać także należy, iż niniejszy artykuł podzielono na dwie zasadnicze części – ogólną (w odniesieniu do ochrony infrastruktury krytycznej i bezpieczeństwa paliwowego państwa) oraz karną (nawiązującą do art. 165 § 1 pkt 3, art. 254a, art. 268a, art. 267, art. 269, art. 269a, art. 278 § 5 oraz 287 k.k.). Część pierwsza ma w założeniu nakreślić specyfikę cyberprzestępczości wymierzonej w infrastrukturę krytyczną, a zatem stanowi wprowadzenie do części dotyczącej przepisów. Wobec konieczności niewykraczania poza dopuszczalną objętość tekstu część pierwsza przedstawia jedynie aspekty definicyjne, zaś część druga dotyczy problemów zdatności wybranych przepisów do penalnej ochrony infrastruktury krytycznej.

Infrastruktura paliwowa jako infrastruktura krytyczna

Kluczowym aktem normatywnym dotyczącym infrastruktury krytycznej w Polsce jest ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3]. Artykuł 3 u.z.k. zawiera katalog definicji legalnych. W art. 3 pkt 2 lit. a u.z.k. legislator wskazuje, że ilekroć w ustawie jest mowa o infrastrukturze krytycznej, należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, zaś infrastruktura krytyczna obejmuje systemy zaopatrzenia w energię, surowce energetyczne i paliwa. Oprócz tych systemów chroniona jest również funkcjonalność systemów łączności, sieci teleinformatycznych, finansowych, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowych, ratowniczych, zapewniających ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (art. 3 pkt 2 lit. b–k u.z.k.). Przywołać należy też definicję z art. 3 pkt 2a u.z.k., gdzie wyróżniona jest europejska infrastruktura krytyczna jako systemy oraz wchodzące w ich skład, powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach, o których mowa w pkt 2 lit. a i h, w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane

[2] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 2021, poz. 1023), dalej: k.k.

[3] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2021, poz. 159), dalej: u.z.k.

na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie.

Podsumowując, trzeba podkreślić, że dwie wskazane definicje nieco się różnią. Z punktu widzenia tematu niniejszego opracowania należy powiedzieć, że na gruncie polskiej infrastruktury krytycznej przedmiotowo chronione są systemy paliw, natomiast w definicji europejskiej infrastruktury krytycznej mowa o paliwach (poprzez odesłanie do definicji z art. 3 pkt 2 lit. a u.z.k.), ale poprzez sprecyzowanie, że chodzi o ropę naftową. Podmiotowo zaś europejska infrastruktura krytyczna dotyczy takich systemów, których zaatakowanie miałoby istotny wpływ na minimum dwa państwa Unii Europejskiej.

W prawie polskim u.z.k. w art. 3 pkt 2 lit. a przesądza, że infrastruktura krytyczna obejmuje systemy zaopatrzenia w energię, surowce energetyczne i paliwa. Z kolei art. 2 ust. 1 pkt 1 ustawy o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym[4] definiuje bezpieczeństwo paliwowe państwa[5]. Współistniejącymi aktami prawnymi, które mają chronić paliwa, są: ustawa o rezerwach strategicznych[6], ustawa o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych[7] czy ustawa o systemie monitorowania i kontrolowania jakości paliw[8]. Natomiast w prawie Unii Europejskiej funkcjonuje dyrektywa Rady 2008/114/WE[9] wyodrębniająca europejską infrastrukturę krytyczną (EIK), do której należy produkcja, rafinacja, przetwarzanie, magazynowanie i przesyłanie rurociągami ropy naftowej.

Prawnokarne aspekty ochrony

Rozważania na temat roli infrastruktury krytycznej i bezpieczeństwa paliwowego w kontekście cyberataków należy osadzić w konkretnych ramach normatywnych

[4] Ustawa z dnia 16 lutego 2007 r. o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym (Dz.U. 2021, poz. 255).

[5] Jako stan umożliwiający bieżące pokrycie zapotrzebowania odbiorców na ropę naftową, produkty naftowe i gaz ziemny w określonej wielkości i czasie, w stopniu umożliwiającym prawidłowe funkcjonowanie gospodarki.

[6] Ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz.U. 2021, poz. 255 ze zm.).

[7] Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz.U. 2020, poz. 2173).

[8] Ustawa z dnia 25 sierpnia 2006 r. o systemie monitorowania i kontrolowania jakości paliw (Dz.U. 2021, poz. 133 ze zm.).

[9] Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE 2008, poz. L 345/75).

i dokonać przeglądu przepisów mogących mieć w takich przypadkach zastosowanie. Pierwszym przepisem karnym, który powinien być przywołany, wydaje się art. 165 § 1 pkt 3 k.k., który przesądza, że kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach powodując uszkodzenie lub unieruchomienie urządzenia użyteczności publicznej, w szczególności urządzenia dostarczającego wodę, światło, ciepło, gaz, energię albo urządzenia zabezpieczającego przed nastąpieniem niebezpieczeństwa powszechnego lub służącego do jego uchylenia, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. We wskazanym katalogu (co prawda otwartym) nie wskazano jednak wprost sektora paliw czy ropy. Autor interpretuje to tak, że sektor ten częściowo zawiera się w słowie *energia* (paliwa i ropa naftowa jako subdostarczyciele energii). Jednak energia została sprecyzowana przy wykładni dalszych przepisów (m.in. art. 278 § 5 k.k.) i nie obejmuje paliw[10] (a na kanwie ustawy, tu: k.k., energia może mieć tylko jedno znaczenie). Wyrazić warto postulat *de lege ferenda*, by do omawianego przepisu dodano wskazanie dotyczące paliw czy ropy naftowej jako odrębnych nośników. Doświadczenie pokazuje, że ich rola mimo stopniowego odchodzenia od nich w segmencie motoryzacji nie będzie malała dynamicznie, a o ich „krytyczności" zaświadczają problemy zaopatrzeniowe będące rezultatem inwazji Rosji na Ukrainę.

O ile w literaturze zaakcentowano, że chronionymi urządzeniami są „wszelkiego rodzaju instalacje, aparatura, armatura, kotły, zbiorniki, pojemniki, pompy, dźwigi, transportery, przyrządy sterujące i kontrolujące oraz każde inne wyposażenie techniczne służące celom użyteczności publicznej, bez którego nie jest możliwe dostarczanie wody, światła, ciepła, gazu lub energii"[11] oraz że karalność dotyczy czynów charakteryzujących się „rozległością zagrożenia dla określonej lub nieokreślonej, ale zawsze większej zbiorowości ludzkiej albo znacznego zasięgu dóbr materialnych"[12], to jednak warte rozważenia wydaje się zintegrowanie definicji infrastruktury krytycznej z przywołanym przepisem. Przy czym podkreślenia wymaga pogląd, że przepis ten sięga szerzej niż wyłącznie bezpośrednia ochrona życia, zdrowia lub mienia, gdyż do przypisania odpowiedzialności wystarczające może być zagrożenie dla bezpieczeństwa powszechnego, uszkodzenie lub unieruchomienie urządzeń użyteczności publicznej[13]. Wydaje się, że do takich urządzeń zaliczyć należy infrastrukturę związaną z wydobywaniem, przetwarzaniem i przesyłem paliw, a przede wszystkim ropy naftowej. Patrząc szerzej, art. 165 k.k. dotyczy sprowadzenia „innego niebezpieczeństwa powszechnego"

[10] Por. postanowienie SN z dnia 9 czerwca 2006 r., sygn. I KZP 14/06, OSNKW 2006, nr 7–8, poz. 67.

[11] R.A. Stefański, *Sprowadzenie innego niebezpieczeństwa powszechnego (art. 165 KK)* [w:] *System Prawa Karnego. Przestępstwa przeciwko państwu i dobrom zbiorowym*, red. L. Gardocki, Warszawa 2018, s. 209.

[12] *Ibidem*.

[13] *Ibidem*.

(tj. innego niż stypizowane w art. 163 czy 173 k.k.). Jednak w definicji infrastruktury krytycznej, o której była mowa w części pierwszej artykułu, wprost przywołane zostały paliwa oraz rurociągi, co uzasadniałoby uspójnienie regulacji na poziomie prawnokarnym.

Kolejnym środkiem ochronnym może być norma prawa karnego z art. 254a k.k., który penalizuje czyn zamachu na urządzenia infrastrukturalne państwa. Czyn ten został określony w rozdziale XXXII k.k. zatytułowanym *Przestępstwa przeciwko porządkowi publicznemu*. Wedle wskazanej regulacji kto zabiera, niszczy, uszkadza lub czyni niezdatnym do użytku element wchodzący w skład sieci wodociągowej, kanalizacyjnej, ciepłowniczej, elektroenergetycznej, gazowej, telekomunikacyjnej albo linii kolejowej, tramwajowej, trolejbusowej lub linii metra, powodując przez to zakłócenie działania całości lub części sieci albo linii, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Artykuł 254a k.k. wprowadzono do polskiego systemu ustawą z dnia 31 sierpnia 2011 r. o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw[14]. Biorąc pod uwagę, że przepis ten jest obecny w polskim prawie już od ponad 10 lat, można powiedzieć, że ustawodawca przewidział natężenie poziomu zagrożenia związanego z atakami na infrastrukturę krytyczną, w tym cyberatakami, gdyż art. 254a k.k. nie wyłącza możliwości penalizacji cyberczynu (*lege non distinguente*) i w tym sensie jest to dyspozycja prawno-karna poprawie i abstrakcyjnie zredagowana (bez rozróżnienie na czyn oraz „cyberczyn"). Jednak również w tym wypadku nie wskazano wprost sieci paliwowych czy naftowych, co analogicznie warte byłoby uzupełnienia. Ocena współczesnych realiów infrastruktury krytycznej każe podać w wątpliwość rozwiązanie prawne, które przykładowo chroni linię trolejbusową, ale nie odnosi się wprost do infrastruktury przesyłowo-magazynowej paliw. Co więcej, art. 254a k.k. może pozostawać w zbiegu kumulatywnym z wyżej wskazanym art. 165 § 1 pkt 3 k.k., jednak żaden z dwóch zbiegających się przepisów nie przesądza o tym, czy infrastruktura paliwowa podlega ochronie, co zdaje się podwajać problem interpretacyjny, jako że oba przepisy stanowią ochronę penalną w nieco odmiennych sytuacjach.

Co ciekawe, wprowadzenie tego uregulowania do polskiego k.k. było podyktowane głównie potrzebą ochrony infrastruktury kolejowej, co zostało podkreślone w uzasadnieniu do nowelizacji. Legislator dostrzegł konieczność odpowiedzi penalnej na problem kradzieży elementów infrastruktury kolejowej, głównie metali szlachetnych, co oprócz przestępstwa kradzieży przekładało się na paraliżowanie połączeń kolejowych (kradzieże części szyn, sygnalizatorów, semaforów, przewodów)[15]. Takie uzasadnienie nowelizacji może dziwić, gdyż równie ważna wydaje się ochrona sieci przesyłowych, choćby przez wzgląd

[14] Dz.U. 2011, nr 217 poz. 1280 ze zm.; J. Piórkowska-Flieger, komentarz do art. 254a k.k. [w:] *Kodeks karny. Komentarz*, red. T. Bojarski, Warszawa 2016, s. 753.

[15] *Ibidem*.

na fakt, że atak na infrastrukturę sieci prowadzić może do nie mniejszego zagrożenia dla funkcjonowania państwa czy społeczeństwa niż katastrofa kolejowa. Transport kolejowy wydaje się być wyłącznie jedną z form do zabezpieczenia dostępności paliw i innych nośników energetycznych.

M. Kalitowski słusznie zwraca uwagę, iż wskazane przez ustawodawcę sieci i linie jako obiekty chronione należy definiować w odniesieniu do ustaw przedmiotowych[16]. Jeżeli chodzi o potencjalne umiejscowienie w tym katalogu paliw (czy ropy naftowej), autor niniejszego opracowania zakłada, że miejsca tego poszukiwać można w „sieci elektroenergetycznej", która sektorowo oznacza instalacje połączone i współpracujące ze sobą, służące do przesyłania lub dystrybucji paliw lub energii, należące do przedsiębiorstwa energetycznego[17]. Tym samym urządzenia magazynowania, przesyłu, transportu czy dystrybucji paliw (ropy naftowej) należałoby potencjalnie rozumieć jako „element" wchodzący w skład sieci, ale już bez procesu pierwotnego – segmentu wrażliwego rynku, jakim jest przemysł petrochemiczny. Wydaje się, że jedynie sieci i linie wskazane bezpośrednio w art. 254a k.k. podlegają na mocy tego przepisu ochronie prawnokarnej. W tym wypadku istnieje wyłączenie ochrona pośrednia (paliwa jako nośnika energii). Warto zarysować analogię: jak trafnie wskazuje Z. Ćwiąkalski, nie będzie przestępstwem w perspektywie tego artykułu k.k. np. niszczenie sieci rowów irygacyjnych w obszarze depresji powierzchniowej, co może doprowadzić do podtopienia miejscowości[18].

Następnie w kontekście cyberprzestępczości wskazać należy na art. 267 k.k. Jak zaznacza F. Radoniewicz, w art. 267 § 1 k.k. przewidziana została odpowiedzialność karna za uzyskanie przez sprawcę bez uprawnienia dostępu do informacji dla niego nieprzeznaczonej przez otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia[19]. Jako przedmiot ochrony art. 267 § 1 k.k. traktować należy poufność informacji, co pozostaje w zbiegu z konstytucyjną gwarancją wolności komunikowania się oraz zabezpieczeniem tajemnicy komunikowania się[20]. Wskazać trzeba, że art. 267 § 1 k.k. penalizuje trzy różne zachowania, które stanowią zamach na bezpieczeństwo systemów informatycznych, czyli: 1) podłączenie się do sieci telekomunikacyjnej; 2) przełamanie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia; 3) ominięcie takiego zabezpieczenia[21]. Jak zauważa

[16] M. Kalitowski, komentarz do art. 254a k.k. [w:] *Kodeks karny. Komentarz*, red. M. Filar, Warszawa 2016, s. 1440–1441.

[17] Art. 3 pkt 11 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. 2023, poz. 295).

[18] Z. Ćwiąkalski, komentarz do art. art. 254a k.k. [w:] *Kodeks karny. Cześć szczególna*, t. II: *Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017, s. 506.

[19] F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu. Sprawy karne" 2013, nr 13, s. 128.

[20] *Ibidem*.

[21] *Ibidem*.

P. Bogacki, zachowanie sprawcy przestępstwa opisanego w art. 267 § 1 k.k. polega na uzyskaniu dostępu do informacji dla niego nieprzeznaczonej, przy czym poprzez pojęcie *uzyskanie* rozumieć należy „otrzymanie, zwykle czegoś pożądanego, czegoś, co było przedmiotem starań, osiągnięcie, zdobycie”[22].

Kluczowym narzędziem do walki z hackingiem pozostaje jednak art. 267 § 2 k.k. Przesądza on, że analogiczną karą, jak w przypadku art. 267 § 1 k.k. (tj. do 2 lat pozbawienia wolności), zagrożony jest czyn, o którym mowa w § 2 tego artykułu penalizującego uzyskanie nieuprawnionego dostępu do całości lub części systemu informatycznego. O ile w art. 267 § 1 k.k. mowa jest o czynie wypełniającym znamiona cyberprzestępstwa również w postaci hackingu poprzez przełamanie albo ominięcie informatycznego zabezpieczenia, o tyle art. 267 § 2 k.k. wprost wskazuje na nieuprawniony dostęp do systemu informatycznego. W literaturze słusznie podnosi się, że konstrukcja art. 267 k.k. dotycząca hackingu jest problematyczna ze względu na fakt, że prawodawca „nie zdecydował się wskazać w jego treści hackingu *sensu stricto* (nieuprawnionego uzyskania informacji z art. 267 § 1 k.k. oraz nieuprawnionego dostępu do systemu informatycznego z art. 267 § 2 k.k.)”[23]. Działania hackerskie polegają na przełamywaniu zabezpieczeń w sieci informatycznej, a więc nie tylko na uzyskaniu dostępu do systemu informatycznego. Można zatem powiedzieć, że art. 267 k.k. łączy w sobie w § 1 i 2 dwie zbliżone, choć nie tożsame kategorie czynów. Zagrożenie ustawowe karą pozostaje jednak na analogicznym poziomie. Warte rozważenia może być zaostrzenie kary dla czynu z art. 267 § 2 k.k wobec art. 267 § 1 k.k. Ustawowe zagrożenie karą analogiczne dla czynu naruszającego tajemnicę korespondencji i czynu dotyczącego „całości systemu informatycznego” nie wydaje się zasadne w toku rozwoju nowych technologii i faktu, że zespolone z systemem informatycznym stają się elementy infrastruktury krytycznej. Docelowo zaś kodeksowe zaostrzenie kary należałoby przewidzieć w formule czynu kwalifikowanego jako działania w zorganizowanej, hackingowej grupie przestępczej[24].

Kolejnym przepisem prawa karnego, który mógłby być rozważany w kontekście cyberataku na elementy infrastruktury krytycznej, jest art. 268a § 1 k.k. Przesądza on, iż kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3. Artykuł 268a k.k. ma chronić bezpieczeństwo informacji w systemach. Chodzi w szczególności o ochronę

[22] P. Bogacki, *Hacking w ujęciu art. 267 KK*, „Monitor Prawniczy” 2013, nr 17, https://czasopisma.beck.pl/monitor-prawniczy/artykul/emhackingem-wujeciu-art267-kk/ (22.04.2023).

[23] D. Brzezińska, *Problematyka regulacji „narzędzi hackerskich” w polskim Kodeksie Karnym*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności” 2016, nr 1(2), s. 56.

[24] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2021, s. 217.

systemów działających w oparciu o tzw. dane informatyczne, które to systemy związane są z użytecznością bądź ochroną takich dóbr prawnych, jak m.in. życie, zdrowie, bezpieczeństwo publiczne czy interesy majątkowe[25]. Podmioty działające w sektorze paliw i ropy naftowej funkcjonują w oparciu o takie systemy[26] i związane są ze wskazanymi dobrami prawnymi, więc wydaje się, że i ten przepis mógłby stanowić potencjalną reakcję karną ze strony państwa w przypadku cyberataku na konkretny podmiot (*vide* bezpieczeństwo publiczne czy interesy majątkowe w zw. z bezpieczeństwem paliwowym państwa). Być może brak w tym miejscu gradacji – np. chodzić może zarówno o przejściowy brak dostępu do poczty elektronicznej osoby fizycznej w sferze prywatnej, jak i uszkadzanie baz danych związanych z funkcjonalnością państwa.

Pytaniem otwartym pozostaje interpretacja wyrażenia *w istotnym stopniu* w kontekście zakłócania lub uniemożliwiania korzystania z danych, które to określenie jawi się jako niefortunne. Po pierwsze, *a contrario* pozwala interpretować, że opisane działanie w natężeniu mniejszym niż istotne nie będzie wyczerpywać znamion czynu, podczas gdy *ratio legis* wymagałoby sformułowania bardziej kategorycznego, zwłaszcza że realne skutki zakłócenia infrastruktury krytycznej związane z takim czynem mogą ujawnić się nawet po latach. Zresztą nawet gdyby nie ujmować tej kwestii pod kątem skutku, niepożądane i sprzeczne z interesem publicznym jest oddziaływanie na infrastrukturę krytyczną w zakresie przetwarzania danych nawet w stopniu nieistotnym. Po drugie, wyrażenie to przedstawia się jako zbędne i „konkurencyjne" wobec systemowego sformułowania *znikoma szkodliwość czynu* (art. 1 § 2 k.k.). Jeśli wskazany cyberczyn ingerowałby w przetwarzanie danych w sposób nieistotny, tak ustalony stan faktyczny znalazłby odzwierciedlenie w kwalifikacji czynu w nawiązaniu do ogólnych norm systemowych i pragmatyki postępowania. To zagadnienie wydaje się warte rozważenia, jako że dotychczas nie stało się przedmiotem zainteresowania komentatorów[27].

W dalszym toku rozważań należy dostrzec art. 269 k.k. penalizujący sabotaż komputerowy oraz art. 269a k.k., który dotyczy uszkodzenia danych informatycznych. Pierwszy z przepisów kryminalizuje w § 1 niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji

[25] W. Wróbel, D. Zając, komentarz do art. art. 268a [w:] *Kodeks karny. Cześć szczególna*, t. II: *Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017, s. 670.

[26] T. Weremij, *Uwarunkowania informatyzacji w zarządzaniu logistyką paliw płynnych w Polsce*, „Logistyka" 2021, nr 5, s. 215–220.

[27] Por. J. Piórkowska-Flieger, komentarz do art. 268a [w:] *Kodeks karny. Komentarz*, red. T. Bojarski, Warszawa 2016, s. 803; M. Kalitowski, komentarz do art. 268a [w:] *Kodeks karny. Komentarz*, red. M. Filar, Warszawa 2016, s. 1472–1474; R.G. Hałas, komentarz do art. 268a [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2019, s. 1325–1326; J. Giezek, komentarz do art. 268a [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, s. 1172–1174.

rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. Z kolei w świetle art. 269 § 2 k.k. tej samej karze co w § 1 podlega ten, kto dopuszcza się czynu w nim określonego, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatyczny. Wydaje się, że dane informatyczne związane z infrastrukturą paliwową mogłyby być uznawane za dane o szczególnym znaczeniu dla obronności kraju. Autor niniejszego opracowania nie dostrzega w tym miejscu pola do kwalifikowania uszkodzenia danych związanych z infrastrukturą paliwową w innych kategoriach z tego przepisu. Wątpliwe pozostaje przy tym sformułowanie związane z bezpieczeństwem w komunikacji, które mogłoby oznaczać zarówno formę komunikacji teleinformatycznej polegającej na przesyłaniu wiadomości, jak i komunikacji w znaczeniu transportu i logistyki, a więc poruszania się. Bezpieczeństwem wydaje się być raczej brak zakłóceń w ruchu lądowym, powietrznym czy wodnym, nie zaś możność nieprzerwanego zapewnienia środków komunikacji ze względu na dostęp do nośników energii i paliw. Kolejne przesłanki są z kolei zupełnie niezwiązane z sektorem paliw. Dane związane z systemem przesyłowym paliw czy infrastrukturą ich przetwarzania również nie wydają się wprost odnosić do obronności kraju, mimo że dostęp do paliw pozwala na użycie pojazdów wojskowych. Obdarzając infrastrukturę paliwową walorem szczególnego znaczenia dla obronności kraju, czyn ten może zyskać charakter *lex specialis* w stosunku do pozostałych cyberczynów albo stanowić komponent opisu czynu (w zw. z art. 165 czy 254a k.k.).

Sektor paliw jako krytycznie istotny będzie jednak kojarzony w pierwszym rzędzie z ogólnymi możliwościami transportu w kraju jako „krwiobiegu gospodarki". Stosowalność wskazanego przepisu jest dalece ocenna, jednak kwalifikowanie sektora paliw jako ważnego z punktu widzenia obrony nie jest wyłączone. Z kolei art. 269a k.k. typizuje przestępstwo polegające na nieuprawnionym, istotnym zakłóceniu pracy systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej poprzez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych. Artykuł ten wydaje się o tyle istotny, że dotyczy systemu informatycznego lub sieci informatycznej jako miejsca, w którym odbywa się przetwarzanie danych (o czym mowa w wyżej wspomnianym art. 268a k.k.). Przedmiotem ochrony jest w tej sytuacji bezpieczeństwo danych informatycznych[28]. Ustawodawca nie poczynił w tym wypadku niecelowego rozróżnienia na systemy informatyczne dotyczące wybranych sektorów rynku, co mogłoby doprowadzić do ryzyka niewyczerpującego scharakteryzowania przedmiotu ochrony. Na tym przykładzie daje się również zauważyć, że ilekroć wskazanie sektora paliwowego (czy naftowego) jest

[28] R.G. Hałas, komentarz do art. 269a [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2019, s. 1327.

pożądane, jeśli ustawodawca formułuje katalog sektorowy (co *de lege ferenda* warto postulować), to przy przestępczości dotyczącej systemów informatycznych nietrafne byłoby dokonywanie jakichkolwiek rozróżnień poza ogólnymi przypadkami zakłócenia pracy sieci i cyberataku na infrastrukturę. Wydaje się przy tym, że art. 268a i 269a k.k. nakładają się zakresowo.

Nadto wskazać należy na art. 287 k.k., który w § 1 stanowi, że kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Jak wskazuje się w piśmiennictwie, w art. 287 k.k. ustawodawca wprowadził nowy typ przestępstwa, które określać można mianem oszustwa komputerowego, gdzie odrębnie spenalizowany został czyn, w którym narzędziem wykorzystywanym do popełnienia przestępstwa przeciwko mieniu jest komputer, co odróżnia ten czyn od tradycyjnej formy oszustwa, gdyż w tym wypadku chodzi o dokonanie ingerencji w maszynę, a dokładniej komputerowe informacje jako zapisy cyfrowe[29]. Artykuł 287 k.k. może także odgrywać istotną rolę przy przypisaniu odpowiedzialności karnej w przypadku ataku na bazę informatyczną w sektorze paliw, o czym decyduje jego poprawnie przewidziana generalność i abstrakcyjność. Za możliwością zastosowania art. 287 k.k. do ochrony infrastruktury paliwowej przemawia doktrynalne rozumienie tego przepisu. Jak wskazuje L. Wilk, w przypadku art. 287 k.k. chodzi o mienie w znaczeniu najbardziej ogólnym, obejmującym zarówno własność, jak i wszelkie inne prawa majątkowe, rzeczowe i obligacyjne, a zatem mienie należy rozumieć jako nazwę zbiorczą – w dowolnej postaci połączone z systemem informatycznym stanowi przedmiot ochrony"[30]. Zwrócić należy uwagę na możliwość kumulatywnego ujęcia czynu stypizowanego w art. 287 k.k. w sytuacji, gdy sprawca uzyska dostęp do systemu, działając w celu uzyskania korzyści majątkowej (np. działał na zlecenie). Wówczas zastosowanie znajdzie kwalifikacja kumulatywna z art. 267 § 1 k.k. w zw. z art. 287 k.k., a zagrożenie karą zwiększy się z 2 lat pozbawienia wolności do lat 5.

Dodać trzeba, że zastosowanie art. 287 k.k. oszustwa komputerowego może mieć coraz bardziej doniosłe znaczenie w świetle ataków hakerskich na systemy informatyczne przedsiębiorstw paliwowych, które dokonywane są w celu osiągnięcia korzyści majątkowej, co miało miejsce np. w Stanach Zjednoczonych. W polskich realiach prawnokarnych kwalifikacja takiego czynu i jego ocena pod kątem wypełnienia znamion byłaby wskazana i możliwa na gruncie art. 287 k.k.

[29] T. Oczkowski, komentarz do art. 287 k.k. [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2018, s. 1739–1740.

[30] L. Wilk, komentarz do art. 287 k.k. [w:] *Kodeks karny. Część szczególna*, t. II: *Komentarz. Art. 222–316*, red. M. Królikowski, R. Zawłocki, Warszawa 2013, s. 648–650.

Podsumowanie

Po pierwsze, pomimo faktu, że niekiedy wskazuje się, iż znaczenie paliw i ropy naftowej może się zmniejszać[31], w obecnych realiach nadal pozostaje podstawowe dla gospodarki[32] i bezpieczeństwa państwa[33]. Co prawda, wydaje się, że w kolejnych dziesięcioleciach dochodzić będzie do zielonej transformacji i eliminowania produkcji samochodów spalinowych z przemysłu motoryzacyjnego, co prognozować można choćby w oparciu o przedstawiony przez Komisję Europejską projekt „Fit for 55"[34], jednak zdarzenie z 7 maja 2021 r., kiedy to zaatakowany został jeden z największych operatorów paliwowo-przesyłowych w Stanach Zjednoczonych, tj. Colonial Pipeline Company[35], dowodzi, że infrastruktura paliwowa (ropy naftowej) wykazuje podatność na ataki hakerskie dokonywane za pomocą internetu. Dość powiedzieć, że ów największy[36] cyberatak na infrastrukturę krytyczną skutkował załamaniem na amerykańskim rynku paliw i doprowadził do braków zaopatrzeniowych na tysiącach stacji[37]. Sytuacja ta może mieć tym donioślejsze znaczenie w perspektywie wojny w Ukrainie i prób „weaponizacji" ropy naftowej przez stronę rosyjską.

Po drugie, zauważyć należy, że pomimo braku bezpośredniego odniesienia w polskim k.k. do ochrony przemysłu rafineryjnego jako zapewniającego bezpieczeństwo paliwowe państwa i będącego tym samym elementem infrastruktury krytycznej, brak takiego odniesienia nie powinien być poczytany za błędny, jednak pożądane wydaje się bezpośrednie odniesienie w polskim k.k. (*de lege ferenda*) do segmentu paliw i ropy naftowej jako sektora krytycznie ważnego. Należy dostrzec, że polski ustawodawca większą ochroną obejmuje sektor energetyczny jako używający paliw i ropy naftowej niż sektor samych paliw i ropy jako poszukiwawczy,

---

[31] Z. Tomczonek, *Światowy rynek ropy naftowej – zasoby, konsumpcja, kierunki przepływu*, „Optimum. Studia ekonomiczne" 2013, nr 4(64), s. 114–115.

[32] S. Pangsy-Kania, *Ropa naftowa jako strategiczny surowiec gospodarki światowej: przyczyny i skutki wahań cen w latach 1970–2017* [w:] *Handel zagraniczny i biznes międzynarodowy we współczesnej gospodarce*, red. M. Maciejewski, K. Wach, Kraków 2017, s. 439–441.

[33] M. Mróz, *Dylematy infrastrukturalnego bezpieczeństwa energetycznego państw tranzytowych ropy naftowej – na przykładzie Polski, Białorusi i Ukrainy*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2020, nr 18, z. 4, s. 77.

[34] A. Słojewska, *Elektryczność i wodór zastąpią ropę naftową*, „Rzeczpospolita" 2021, nr 162(12014), s. A16.

[35] P. Rosa-Aquino, C. Danner, *What We Know About the Colonial Pipeline Shutdown*, https://nymag.com/intelligencer/article/what-we-know-about-the-colonial-pipeline-shutdown-updates.html (22.04.2023).

[36] M. Kania, *Amerykańska ropa zakładnikiem hakerów. Czy chodziło tylko o pieniądze?*, https://wyborcza.biz/biznes/7,177150,27068072,amerykanska-ropa-zakladnikiem-hakerow.html (22.04.2023).

[37] P. Kubiak, *USA. Atak hakerski na Colonial Pipeline. Służby odzyskały prawie 64 bitcoiny*, https://wiadomosci.wp.pl/usa-atak-hakerski-na-colonial-pipeline-sluzby-odzyskaly-prawie-64-bitcoiny-6648369564728032a (22.04.2023).

przetwórczy i magazynujący, co nie oznacza braku ochrony infrastruktury paliwowej na podstawie wskazanych norm prawa karnego, które pozostają właściwe w zakresie zwalczania cyberprzestępczości, tym samym nie istnieje w tym zakresie spójność z ustawową definicją infrastruktury krytycznej.

Po trzecie, wydaje się, że ani fakt stosunkowo nowej ustawy o rezerwach strategicznych, która na podstawie art. 31 ust. 1 pkt 8 do zadań Agencji[38] przekazuje tworzenie i utrzymywanie zapasów agencyjnych ropy naftowej i paliw na zasadach określonych w ustawie o zapasach ropy naftowej i produktów naftowych oraz wykonywanie innych obowiązków wynikających z tej ustawy, ani fakt pozostawienia przez Skarb Państwa wpływów w spółce paliwowej[39] nie wydają się gwarantami bezpieczeństwa paliwowego, gdyż jako takie są faktem ekonomicznym i wypadkową działania państwa w sferze *imperium* i *dominium*; jednak biorąc pod uwagę regulacje prawnokarne, widać, iż na podstawie obecnie obowiązującego k.k. możliwe pozostaje przypisanie odpowiedzialności karnej za cyberataki na infrastrukturę krytyczną, choć niekiedy nie jest ono szczególnie wyodrębnione i wskazane wprost (nazewniczo i sektorowo).

Bibliografia

Brzezińska D., *Problematyka regulacji „narzędzi hackerskich" w polskim Kodeksie Karnym*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2016, nr 1(2).

Ćwiąkalski Z., komentarz do art. art. 254a [w:] *Kodeks karny. Cześć szczególna*, t. II: *Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017.

Długosz T., *Ochrona infrastruktury krytycznej w sektorach energetyki sieciowej*, Warszawa 2015.

Gałązka M., komentarz do art. 278 [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2019.

Giezek J., komentarz do art. 268a [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021.

Hałas R.G., komentarz do art. 268a [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2019.

Hołyst B., *Kryminologia*, Warszawa 2016.

Kalitowski M., komentarz do art. 254a [w:] *Kodeks karny. Komentarz*, red. M. Filar, Warszawa 2016.

Mróz M., *Dylematy infrastrukturalnego bezpieczeństwa energetycznego państw tranzytowych ropy naftowej – na przykładzie Polski, Białorusi i Ukrainy*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2020, nr 18(4).

Oczkowski T., komentarz do art. 287 [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2018.

OECD, *The Size and Sectoral Distribution of State-Owned Enterprises*, Paris 2017.

[38] Rządowa Agencja Rezerw Strategicznych.

[39] Mowa przede wszystkim o przedsiębiorstwie Polski Koncern Naftowy Orlen S.A., gdzie Skarb Państwa posiada 27,52% udziału w kapitale podstawowym i tym samym w ogólnej liczbie głosów, zachowując 117 710 196 akcji. Zob. OECD, *The Size and Sectoral Distribution of State-Owned Enterprises*, Paris 2017, s. 28.

Pangsy-Kania S., *Ropa naftowa jako strategiczny surowiec gospodarki światowej: przyczyny i skutki wahań cen w latach 1970–2017* [w:] *Handel zagraniczny i biznes międzynarodowy we współczesnej gospodarce*, red. M. Maciejewski, K. Wach, Kraków 2017.
Piórkowska-Flieger J., komentarz do art. 254a [w:] *Kodeks karny. Komentarz*, red. T. Bojarski, Warszawa 2016.
Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu. Sprawy karne" 2013, nr 13.
Sadowski J., *Cybernetyczny wymiar współczesnych zagrożeń*, „Studia nad Bezpieczeństwem" 2017, nr 2.
Słojewska A., *Elektryczność i wodór zastąpią ropę naftową*, „Rzeczpospolita" 2021, nr 162(12014).
Stefański R.A., *Sprowadzenie innego niebezpieczeństwa powszechnego (art. 165 KK)* [w:] *System Prawa Karnego. Przestępstwa przeciwko państwu i dobrom zbiorowym*, red. L. Gardocki, Warszawa 2018.
Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2021.
Tomczonek Z., *Światowy rynek ropy naftowej – zasoby, konsumpcja, kierunki przepływu*, „Optimum. Studia ekonomiczne" 2013, nr 4(64).
Weremij T., *Uwarunkowania informatyzacji w zarządzaniu logistyką paliw płynnych w Polsce*, „Logistyka" 2021, nr 5.
Wilk L., komentarz do art. 287 k.k. [w:] *Kodeks karny. Część szczególna*, t. II: *Komentarz. Art. 222–316*, red. M. Królikowski, R. Zawłocki, Warszawa 2013.
Wróbel W., Zając D., komentarz do art. art. 268a [w:] *Kodeks karny. Cześć szczególna*, t. II: *Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, Warszawa 2017.

Streszczenie

Celem niniejszego artykułu jest analiza problematyki cyberprzestępczości z punktu widzenia ochrony infrastruktury paliwowej jako infrastruktury krytycznej. Przyjętą metodą badawczą była metoda dogmatycznoprawna. Analizowano przepisy Kodeksu karnego i innych aktów prawnych. Infrastruktura paliwowa nadal ma kluczowe znaczenie dla bezpieczeństwa państwa, choć jej rola może się zmniejszać. Hipotezą główną było założenie, że infrastruktura paliwowa jest w ujęciu prawnokarnym chroniona wyłącznie przez pryzmat ogólnego katalogu przestępstw. Wobec tego należy zweryfikować odporność prawa karnego na naruszenie infrastruktury paliwowej. Ustalenia zawarte w tekście są szczególnie ważne ze względu na znaczenie dla obronności państwa w kontekście sytuacji nadzwyczajnych, takich jak np. wrogie działania hybrydowe mające postać cyberataków. Tym samym kluczowe jest zabezpieczenie państwowej infrastruktury krytycznej przez sankcje prawnokarne.

Słowa kluczowe: cyberprzestępczość, infrastruktura krytyczna, infrastruktura paliwowa

THE SUITABILITY OF CRIMINAL LAW REGULATIONS TO COMPREHENSIVELY PROTECT FUEL CRITICAL INFRASTRUCTURE FROM CYBERCRIME

Summary

The purpose of this article is to analyse the issue of cybercrime from the point of view of protecting fuel infrastructure as critical infrastructure. The research method adopted is the dogmatic-legal

method. The provisions of the Criminal Code and other legal acts are analysed. Fuel infrastructure continues to be critical to state security, although its role may be diminishing. The main hypothesis is that fuel security is protected in criminal law terms only through the prism of a general catalogue of offences. In view of this, the resilience of criminal law to violations of fuel infrastructure needs to be reviewed. The findings of the text are particularly important due to the relevance for state defence in the context of emergency situations, such as, for example, hostile hybrid actions conducted by cyber-attacks. Thus, it is crucial to safeguard state critical infrastructure through criminal law sanctions.

Keywords: cybercrime, critical infrastructure, fuel infrastructure