Recenzja monografii: *Filip Radoniewicz*, Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warszawa 2016

dr *Piotr Siemkowicz*[1]

Monografia autorstwa *F. Radoniewicza*, pt. Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, jest ciekawym opracowaniem, w którym autor starał się w sposób możliwie pełny przedstawić najistotniejsze zagadnienia związane z pojęciem hackingu oraz innych przestępstw skierowanych przeciwko bezpieczeństwu danych komputerowych i systemów informatycznych w ujęciu praktycznym i karnoprawnym.

Już pierwszy rozdział pt. Hacking – zagadnienia ogólne, stanowi pogłębione spojrzenie na rozwój technologii komputerowej, począwszy od lat 40. ubiegłego wieku aż do czasów współczesnych. Autor sygnalizuje przy tym technologiczne uwarunkowania i przyczyny powstawania sieci komputerowych – zarówno lokalnych sieci LAN w standardzie Ethernet, jak i genezę powstania sieci Internet, wywodzącej swoje korzenie od sieci ARPANet. W rozdziale tym przedstawiono genezę pojęcia terminu „hacker" i „hacking", przy czym autor wskazuje na ewolucję omawianych terminów, obecnie (odmiennie niż przed kilkoma dekadami) postrzeganych zazwyczaj w kontekście negatywnym.

Istotną zaletą rozdziału pierwszego jest niewątpliwie przedstawienie – niejako w „pigułce", podstawowych pojęć informatycznych oraz technicznych, dotyczących budowy, struktury i funkcjonowania zarówno urządzeń komputerowych, jak i sieci komputerowych. Podkreślić przy tym należy, że w większości wypadków opracowania dotyczące cyberprzestępczości pomijają tego rodzaju wprowadzenie techniczne, co bez wątpienia uznać należy za błąd.

W omawianym rozdziale poddano także analizie techniczne aspekty działań hackerskich (zarówno na etapie przygotowawczym, ataku właściwego, jak i tzw. zacierania śladów po przeprowadzonym ataku) dokonywanych głównie w środowisku sieciowym, jak też omówiono najczęściej spotykane rodzaje ataków hackerów. Autor przedstawia na wstępie – w ślad za innymi cytowanymi w przypisach autorami, klasyfikację ataków hackerskich między innymi na podstawie: kryterium stopnia interakcji sprawcy z atakowanym systemem (ataki pasywne i aktywne), kryterium źródła ataku (ataki lokalne i zdalne) oraz z uwagi na kryterium liczby zaangażowanych komputerów (ataki bezpośrednie i rozproszone). Autor zamieścił także w swojej publikacji propozycję przyjęcia dla systematyzacji ataków hackerskich kryterium zamiaru sprawy – wyróżniając w tym zakresie ataki umyślne i nieumyślne. Ta ostatnia klasyfikacja może jednak budzić pewne wątpliwości, a to z uwagi na uznanie, że atak hackerski może mieć *de facto* charakter nieumyślny. Warto zauważyć, że przestępstwa o charakterze hackerskim, w tym zwłaszcza z rozdziału XXXIII Kodeksu karnego, dla ich realizacji wymagają umyślności, a tym samym działania sprawcy w zamiarze bezpośrednim lub co najmniej ewentualnym. Tym samym wskazane przez autora na s. 76 niniejszej monografii opisy, iż: „wbrew pozorom wiele ataków ma taki właśnie charakter, jest dziełem przypadku lub wynika ze zwykłej ludzkiej nieostrożności", a także dalej, iż „przykładowo, większość wirusów rozprzestrzenianych jest przez sieć przez nieświadomych tego użytkowników. Sieć może też zostać unieruchomiona przez użytkownika eksperymentującego z oprogramowaniem" – należałoby raczej zakwalifikować jako „incydenty sieciowe", nie zaś ataki hackerskie *sensu stricto*. Reasumując, użycie sformułowania „atak" do zachowania nieumyślnego – które faktycznie, co do zasady, nie zrealizuje znamion przestępstwa zaliczanego do ogólnej grupy przestępstw hackerskich, wydaje się nieuprawnione.

Autor opisuje następnie w podrozdziale 1.3 najczęściej spotykane rodzaje ataków hackerskich takie jak: posłużenie się złośliwym oprogramowaniem w postaci m.in. koni trojańskich, exploitów, rootkitów czy też wirusów komputerowych, *sniffing*, *spoofing* i jego odmiany, *session hijacking*, *pharming* i *drive-by pharming*, *man-in-the-middle*, wykorzystanie luk i błędów w aplikacjach (przepełnienie buforów, SQL Injection oraz ataki XSS), łamanie haseł, *phishing*, ataki odmowy usługi – dostępu (DoS, DDoS i DRDoS), bomby e-mailowe oraz *bluejacking* i *bluehacking*. Autor jako jeden z rodzajów ataków hackerskich wymienia także stosowane przez hackerów socjotechniki (inżynierii społecznej), w tym tzw. odwrotną socjotechnikę. Pogląd ten może budzić pew-

[1] Autor wykonuje zawód adwokata. W ramach swoich zainteresowań naukowych autor zajmuje się prawem karnym, w tym w szczególności problematyką szeroko rozumianej przestępczości komputerowej i internetowej.

ne wątpliwości z uwagi na to, iż stosowane przez hackerów metody socjotechniczne, zmierzające do wykorzystania tzw. słabego ogniwa systemu (a więc naiwności czy też lekkomyślności pracownika – użytkownika systemu), najczęściej w celu zdobycia loginów, haseł dostępu i uzyskania istotnych dla przyszłego ataku informacji o systemie, zazwyczaj mają charakter czynności przygotowawczych. Tym samym pomimo że czynności te faktycznie często warunkują późniejszą skuteczność ataku hackerskiego, zazwyczaj samym atakiem sieciowym jeszcze nie są, chyba że mają charakter powiązany z inną metodą hackerską – w tym głównie *pharmingiem* lub *phishingiem* – i są dokonywane w celu skierowania użytkownika np. na fałszywą stronę WWW instytucji bankowej po to, aby wyłudzić wpisywane na niej hasła i loginy.

Niezależnie od wskazanych powyżej uwag, sposób zaprezentowania przez autora poszczególnych rodzajów działań hackerskich, w tym głównie o charakterze destrukcyjnym, uznać należy za pełny i przejrzysty.

W omawianym podrozdziale przedstawiono także wiele informacji praktycznych, począwszy od szczegółowego nazewnictwa i sposobu działania złośliwego oprogramowania, a także potencjalnych skutków użycia takich programów komputerowych przez hackera. Autor w szczególności poddał analizie kilka rodzajów wirusów komputerowych w kontekście sposobu ich działania, cech charakterystycznych oraz umiejscowienia. Szczegółowe rozważania dotyczą wykorzystania w inwazyjnych działaniach hackerskich koni trojańskich i innych odmian złośliwego oprogramowania, przy czym autor sposób działania tych programów komputerowych przedstawił na podstawie praktycznych przykładów.

Do złośliwego oprogramowania autor zalicza także nie bez racji pliki *cookies* i *tracking cookies* (ciasteczka śledzące), które co do zasady nie mają charakteru szkodliwego lub destrukcyjnego dla systemów i danych komputerowych, służą jednak do gromadzenia danych wrażliwych dotyczących użytkownika odwiedzającego daną stronę WWW, a w przypadku *tracking cookies* także do obserwowania działań podejmowanych przez użytkownika w sieci, co służy w efekcie dopasowaniu reklam do gustu i zainteresowań użytkownika. W rzeczywistości nie można jednak wykluczyć, że dane zdobyte we wskazany sposób mogą być także wykorzystane w celach przestępczych, w tym także do podszywania się pod cudzą tożsamość.

Także szczegółowa analiza poszczególnych rodzajów ataków hackerskich (s. 89–113) dokonana przez autora jawi się jako przedstawiona w sposób profesjonalny oraz przydatny z punktu widzenia celu, dla którego przedmiotowa monografia została przygotowana. Zastrzeżenia budzi jedynie kilkukrotne odwoływanie się w przypisach podrozdziału 1.3 do wpisów opublikowanych w Wikipedii. Z natury rzeczy trudno uznać Wikipedię za źródło o charakterze naukowym, a zarazem w pełni wiarygodne. Poszczególne hasła opracowywane są bowiem w jej ramach przez często bliżej nieokreślonych autorów i pochodzą niekiedy z wątpliwych naukowo źródeł. Tym samym odwołania w przypisach: Nr 182 (w zakresie dotyczącym *bluejackingu*), Nr 186, 187, 189, 190 (w zakresie dotyczącym systemów wykrywania ataków) oraz Nr 194 i 195 (w zakresie dotyczącym programów wykorzystywanych w informatyce śledczej – EnCase i PTK_Forensics) bezpośrednio do polskiej i angielskiej edycji Wikipedii wydają się istotnym mankamentem publikacji o charakterze *stricte* naukowym.

Rozdział drugi poświęcony został natomiast wprowadzeniu w problematykę przestępczości komputerowej. Autor przedstawia w nim ogólne pojęcie przestępstwa komputerowego, sygnalizując zarazem, że dotychczas żaden ustawodawca nie zdecydował się na wprowadzenie do systemu prawnego definicji legalnej przestępstwa komputerowego, a spotykane dotychczas próby zdefiniowania tego pojęcia mają wyłącznie miejsce w ramach doktryny prawa karnego. Autor przedstawia także w tym zakresie własną „roboczą" definicję przestępstwa komputerowego (cyberprzestępstwa) jako każdego nielegalnego działania skierowanego przeciwko systemom komputerowych, sieciom komputerowym lub danym komputerowym, albo takiego, w którym system komputerowy lub sieć komputerowa są narzędziem służącym jego popełnieniu.

W dalszej części rozdziału drugiego autor, poza sygnalizacją zagrożeń oraz nowych wyzwań związanych z pojawieniem się przestępczości komputerowej oraz krótkim zarysem historii kryminalizacji tego zjawiska, poddaje również analizie podstawowe pojęcia istotne z punktu widzenia znamion czynów o charakterze hackingu, takie jak: „informacja", „dane", „program komputerowy", a także „poufność", „integralność" i „dostępność danych komputerowych".

Rozdział trzeci poświęcony został natomiast inicjatywom międzynarodowym mającym na celu zwalczanie cyberprzestępczości. Autor poddał w przedmiotowym rozdziale analizie wiele działań i instytucji międzynarodowych bezpośrednio wiążących się z przeciwdziałaniem przestępczości komputerowej i internetowej. W rozdziale tym autor pogłębionej analizie poddaje w szczególności przepisy Konwencji o cyberprzestępczości – przyjętej przez Komitet Ministrów Rady Europy 8.11.2001 r., a otwartej do podpisu 23.11.2001 r. w trakcie Międzynarodowego Kongresu w sprawie cyberprzestępczości w Budapeszcie.

Rozdział czwarty recenzowanej monografii poświęcony został z kolei zagadnieniom cyberprzestępczości w ramach prawa Unii Europejskiej. Autor przedstawił w nim poszczególne akty prawa europejskiego – począwszy od decyzji Rady 92/242/WE z 31.3.1992 r. w dziedzinie bezpieczeństwa systemów informatycznych, skończywszy na komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM (2009) 149 z 30.3.2009 r. w sprawie ochrony krytycznej infrastruktury informatycznej „Ochrona Europy przed

zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności" wraz z załączonym do niego raportem na temat bezpieczeństwa sieciowego.

Ostatnia część tego rozdziału poświęcona została natomiast szczegółowej analizie decyzji ramowej Rady Unii Europejskiej Nr 2005/222 z 24.2.2005 r. w sprawie ataków na systemy informatyczne oraz późniejszej i analogicznej zakresowo dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z 12.8.2013 r. dotyczącej ataków na systemy informatyczne oraz uchylającej decyzję ramową Rady 2005/222/WSiSW. Przedmiotowa analiza, mająca częściowo charakter porównawczy w kontekście uprzednich aktów prawa międzynarodowego – w tym zwłaszcza Konwencji o cyberprzestępczości, przeprowadzona została przez autora w sposób pełny i niebudzący zastrzeżeń.

Rozdział piąty recenzowanej monografii pt. Przestępstwa przeciwko danym komputerowym i systemom informatycznym w polskim Kodeksie karnym, został poświęcony omówieniu poszczególnych typów przestępstw z rozdziału XXXIII oraz stanowi on tym samym formę komentarza autorskiego.

W „uwagach wstępnych" zamieszczonych przez Autora na początku rozdziału piątego zwrócono uwagę na kilka istotnych kwestii mających znaczenie dla dokonywania prawidłowej wykładni gramatycznej (językowej) przepisów rozdziału XXXIII Kodeksu karnego. W szczególności słusznie podnosi autor, iż w sytuacji gdy dane określenie odnoszące się do terminologii bezpośrednio związanej z katalogiem przestępstw z art. 267–269b KK jest nieostre lub wieloznaczne, a jego znaczenie nie jest powszechnie zrozumiałe, istnieje konieczność ustalenia właściwego (nowego) znaczenia tego pojęcia w ustawie lub w innym akcie prawnym. Niestety, zdarza się – jak słusznie podkreśla autor – że ustawodawca próbuje często znaleźć polski odpowiednik terminologiczny danego pojęcia zapożyczonego z aktów prawa międzynarodowego w trakcie procesu dostosowywania polskiego prawa do standardów światowych bądź europejskich, na co trafnie przywołanym przez autora przykładem jest dosyć nieszczęśliwy przekład pojęcia *interface* zapożyczonego z dyrektywy Rady 1991/250/EWG z 14.5.1991 r. w sprawie ochrony prawnej programów komputerowych, gdzie w rozdziale 7 ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych przetłumaczono to pojęcie jako „łącze".

Słuszne były także uwagi autora (poczynione na bazie poprzednio obowiązującej regulacji prawnej w tym zakresie), iż posługiwanie się uprzednio przez ustawodawcę w rozdziale XXXIII Kodeksu karnego dwoma odmiennymi pojęciami „system informatyczny" (w art. 267 § 2 KK) oraz „system komputerowy" (w art. 269a i 269b § 1 KK – w ich brzmieniu sprzed 27.4.2017 r.) wydawało się działaniem zamierzonym i faktycznie odnosiło się do zakresu stosowania ww. regulacji. Jak bowiem celnie wskazano, zakres przedmiotowy pojęcia „system komputerowy" jest znacznie węższy niż zakres pojęcia „system informatyczny" – pierwszy obejmuje faktycznie pojedynczy host w rozumieniu komputera, telefonu komórkowego, smartfona, dekodera, drugi zaś oznacza z reguły połączone ze sobą co najmniej dwie jednostki (hosty) działające w sieci. W tym kontekście, zdaniem autora, nie jest możliwe zamienne stosowanie pojęć „systemu komputerowego" i „sytemu informatycznego".

Uwagi te obecnie, ze względu na nowelizację art. 269a oraz 269b § 1 KK dokonaną ustawą z 23.3.2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw[2], a także z uwagi na usunięcie z tych przepisów pojęcia „systemu komputerowego" i „sieci informatycznej" oraz zastąpienia ich nowymi pojęciami „systemu informatycznego", „systemu teleinformatycznego" oraz „sieci teleinformatycznej", utraciły swoją aktualność.

Ciekawymi jawią się rozważania autora poczynione na kanwie art. 267 § 2 KK, a dotyczące skutków uzyskania przez sprawcę dostępu do niezabezpieczonej sieci bezprzewodowej. Zwrócono w tym zakresie uwagę na zjawiska określane jako *wardriving* oraz *piggybacking*. Pierwsze z nich – polegające na poszukiwaniu za pomocą urządzenia (laptopa, notebooka) wyposażonego w kartę sieciową WLAN niezabezpieczonych sieci bezprzewodowych – jak słusznie zauważa autor, nie wyczerpuje znamion przestępstwa, jeśli nie wiąże się z próbą uzyskania dostępu do sieci. Czyn z art. 267 § 2 KK byłby w tej sytuacji zrealizowany dopiero wówczas, gdyby sprawca uzyskał dostęp do danych informatycznych przetwarzanych w tej sieci bezprzewodowej. Oczywiste jest przy tym, że dla bytu przestępstwa z art. 267 § 2 KK nie ma znaczenia, czy sprawca w celu uzyskania takiego dostępu przełamuje zabezpieczenia. W sytuacji jednak gdy sprawca w celu uzyskania dostępu do danych informatycznych takie zabezpieczenia złamie lub ominie (przy założeniu, że zabezpieczenia takie w ogóle zostały zastosowane), a następnie uzyska informację, do której nie jest uprawniony, to wówczas – jak celnie wskazuje autor – zrealizuje znamiona czynu z art. 267 § 1 KK.

W odniesieniu do zjawiska *piggybackingu* – związanego z uzyskaniem dostępu do systemu informatycznego w wyniku wykorzystania uprawnień innego użytkownika – autor trafnie zauważa, że zachowanie takie realizują także ataki typu *session hijacking* oraz *man-in-the-middle*, które powinny być kwalifikowane jako przestępstwa z art. 267 § 3 KK. W pełni należy zgodzić się przy tym z dalszymi rozważaniami poczynionymi w tym zakresie, iż w przypadku *piggybackingu* w ramach sieci Wi-Fi, polegającego na uzyskaniu nieuprawnionego dostępu do sieci bezprzewodowej (zwłaszcza w przypadku gdy nie była ona zabezpieczona)

[2] Dz.U. poz. 768.

– wyłącznie w celu korzystania z usług sieciowych na rachunek konkretnego hosta z takiej sieci, poza faktycznym efektem w postaci spadku wydajności sieci (co w przypadku istotnego zakłócenia jej funkcjonowania można byłoby ewentualnie kwalifikować jako czyn z art. 269a KK), trudno będzie przypisać sprawcy takiego działania realizację czynu o znamionach przestępstwa. Jak słusznie zwraca na to uwagę autor, w niektórych przypadkach może jednak dojść do określonych konsekwencji finansowych po stronie ofiary takiego działania, w szczególności gdy sprawca wykorzysta bezprawne uzyskanie dostępu do ww. sieci Wi-Fi do transferu lub pobierania znacznej ilości danych. Rodzić to może po stronie legalnego użytkownika określone konsekwencje finansowe w postaci zwiększonego rachunku za transfer, który został wykorzystany *de facto* przez sprawcę. Zauważyć przy tym należy, że do opisywanej sytuacji nie będzie mógł z oczywistych względów znaleźć zastosowania art. 285 § 1 KK – sankcjonujący tzw. kradzież impulsów telefonicznych, a to z uwagi na użycie przez ustawodawcę we wskazanym przepisie pojęcia „uruchomienia na cudzy rachunek impulsów telefonicznych", co w żadnym zakresie nie może być utożsamiane z transferem danych informatycznych. Tym samym z uwagi na pominięcie przez ustawodawcę w treści art. 269a KK elementu „wyrządzenia szkody majątkowej", w przypadku gdy łączy się ona z transmisją danych informatycznych dokonywanych bez uprawnienia przez sprawcę za pośrednictwem sieci Wi-Fi, faktycznie w większości wypadków opisywane powyżej działanie sprawcy nie będzie podlegało możliwości ścigania na gruncie ustawy karnej.

Za słuszne należy także uznać spostrzeżenie przedstawione w ramach omawianego rozdziału (s. 305), że art. 267 § 3 KK kryminalizuje jedynie przechwytywanie danych komputerowych w czasie ich przesyłania (w czasie rzeczywistym), co z oczywistych względów oznacza, że w przypadku uzyskania przez sprawcę danych przechowywanych np. na serwerze czy w prywatnym komputerze właściwa będzie kwalifikacja z art. 267 § 1 KK lub z art. 267 § 2 KK.

Za istotne uznać należy także spostrzeżenia przedstawione na s. 309 recenzowanej monografii, iż za niedopatrzenie ustawodawcy uznać należy brak w ramach regulacji art. 267 KK typu kwalifikowanego omawianego przestępstwa – a mianowicie czynu, który miałby polegać na posłużeniu się przez sprawcę w celu ujawnienia określonych informacji środkami masowego przekazu, na zasadach analogicznych do czynu z art. 212 § 2 KK. Oczywiste jest bowiem, że także dane uzyskane w ramach działań realizujących znamiona czynu z art. 267 § 1–3 KK mogą być następnie rozpowszechnione za pośrednictwem sieci Internet, w tym np. na stronie internetowej, w ramach portalu społecznościowego lub serwisu o zasięgu globalnym. Tym samym ściganie takich czynów jedynie w ramach art. 267 § 4 KK – sankcjonującego ujawnienie innej osobie informacji uzyskanej w sposób określony w art. 267 § 1–3 KK, wydaje się daleko niewystarczające. Autor słusznie przytacza przy tym przykład działalności portalu Wikileaks.

W odniesieniu do czynu z art. 268 § 1 i 2 KK autor zauważa, że zniszczenie jednej z kopii zapisanej informacji (w sytuacji gdy użytkownik ma nadal dostęp do tych informacji w ramach innych kopii) nie wypełnia znamion omawianego przestępstwa. W tym zakresie podzielony został także pogląd *A. Adamskiego*, że znamion tego czynu nie wypełnia zachowanie sprawcy, który niszczy nośnik danych, w sytuacji gdy dysponent tych danych posiada kopię zapasową, oraz że zachowanie takie można kwalifikować jedynie jako usiłowanie czynu z art. 267 § 1 lub 2 KK.

W zakresie czynu z art. 268a § 1 lub 2 KK autor podejmuje m.in. polemikę z reprezentowanym w doktrynie poglądem, że wskazane przepisy dotyczą danych zgromadzonych w formie baz danych. Przeciwstawiając się temu poglądowi, autor wskazuje, że pojęcie bazy danych nie jest tożsame z pojęciem zbioru danych, przy czym zbiór danych w sensie informatycznym musi spełniać kilka dodatkowych kryteriów, aby można było uznać go za bazę danych. Pogląd ten, który w mojej ocenie należy podzielić, autor rozwija dodatkowo w przypisach Nr 772 i 773, systematyzując pojęcia baz danych oraz zbioru danych. Dodatkowo w przedmiotowym podrozdziale słusznie zwraca się uwagę na nieprecyzyjność art. 268a § 1 KK, a to w kontekście wątpliwości rodzących się na kanwie postawionego tam pytania o to, co faktycznie jest przedmiotem wykonawczym kryminalizowanych zachowań opisanych w tym przepisie. Przepis ten w swojej początkowej treści stanowi bowiem, że „kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych", co z oczywistych względów rodzi pytanie, czy przedmiotem wykonawczym tego czynu jest „dostęp do danych informatycznych" czy też „dane informatyczne". Autor przychyla się przy tym do stanowiska, że wskazanym przedmiotem wykonawczym są „dane informatyczne". Stanowisko to należy uznać za przekonujące – a to z uwagi na wykładnię logiczną ww. przepisu. W sytuacji bowiem uznania (zgodnie z literalnym brzmieniem przepisu), iż przedmiotem wykonawczym czynu z art. 268a § 1 KK jest „dostęp do danych informatycznych", należałoby uznać wszakże, że możliwe jest „niszczenie, uszkadzanie, usuwanie bądź zmienianie" takiego „dostępu" do przedmiotowych danych informatycznych, co z oczywistych względów jest niemożliwe. Niszczyć, uszkadzać, usuwać bądź zmieniać można bowiem wyłączenie dane informatyczne – po wcześniejszym uzyskaniu do nich dostępu.

W podrozdziale ósmym rozdziału piątego autor omawia czyn z art. 269 KK (sabotażu informatycznego), zauważając zarazem, że z uwagi na zdecydowanie wyższe znaczenie informacji chronionych przez art. 269 § 1 KK w porównaniu z informacjami podlegającymi ochronie na podstawie

art. 268 § 2 KK oraz podobieństwo pozostałych znamion czynów kryminalizowanych przez te przepisy, przy jednoczesnej różnicy w wysokości zagrożenia karą i środkami karnymi, przestępstwo z art. 269 § 1 KK uważa się za typ kwalifikowany w stosunku do przestępstw z art. 268 § 2 KK. Dodatkowo słusznie podkreśla się w ramach przedmiotowego omówienia, iż nie stanowi przestępstwa określonego w art. 269 § 2 KK takie zachowanie, które prowadzi do zniszczenia lub wymiany nośnika danych albo do zniszczenia lub uszkodzenia urządzenia służącego do przetwarzania, gromadzenia lub przekazywania danych, jeżeli jednocześnie sprawca nie zniszczył, nie uszkodził, nie usunął lub nie zmienił zapisu danych o szczególnym znaczeniu w rozumieniu tego przepisu bądź nie doprowadził do zakłócenia lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Autor trafnie zauważa jednak, że w przypadku gdy sprawca wiedział, jakie jest przeznaczenie urządzeń będących przedmiotem jego czynu – możliwe będzie zakwalifikowanie działania sprawcy jako usiłowania, przy czym w jego ocenie podobna sytuacja zajdzie wówczas, gdy czyn sprawcy skutkować będzie jedynie uszkodzeniem nośnika danych, a nie jego zniszczeniem.

W uwagach dotyczących art. 269a KK (zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej) autor wysuwa pogląd, iż wskazany przepis znajduje zastosowanie do wszystkich zamachów na bezpieczeństwo sieci o charakterze logicznym – a więc np. ataków odmowy usługi DoS, rozproszonej odmowy usługi DDoS lub polegających na manipulacji danymi wejściowymi, a tym samym ma on charakter szczególny w stosunku do art. 268a § 1 KK – istotnie ograniczając w związku z tym jego znaczenie i redukując jego zastosowanie do zamachów na dane informatyczne lub ewentualnie zamachów fizycznych na bezpieczeństwo sieci. W przypadku natomiast gdy sprawca wyrządzi znaczną szkodę, której możliwość przewidywał i na to się godził, odpowie za czyn z art. 268a § 2 KK.

W uwagach dotyczących czynu z art. 269b § 1 KK autor słusznie zwraca uwagę, iż przepis ten jest skonstruowany wadliwie, w tym poprzez brak wskazania w jego treści hackingu *sensu stricto* – a więc nieuprawnionego uzyskania informacji z art. 267 § 1 KK oraz nieuprawnionego dostępu do systemu informatycznego z art. 267 § 2 KK.

Dalsze uwagi autora co do oceny działań twórcy programu spełniającego faktycznie kilka funkcji, który może zostać następnie użyty przez inną osobę w celach przestępczych, z uwagi na nowelizację dokonaną ww. nowelizacją z 23.3.2017 r., utraciły, jak się wydaje, swoją aktualność. W szczególności bowiem z uwagi na wprowadzenie art. 269b § 1a KK stanowiącego, że nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia, brak jest obecnie możliwości pociągnięcia do odpowiedzialności karnej osoby, która wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy o cechach opisanych w art. 269b § 1 KK, jednakże czyni to jedynie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.

Podobny charakter ma również dodany tą samą ustawą art. 269c KK, który stanowi, iż nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a KK, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Dalsza część rozdziału piątego (podrozdział 5.11) poświęcona została omówieniu często poruszanej w doktrynie przedmiotu problematyki zbiegu przepisów i przestępstw w zakresie czynów rozdziału XXXIII – zarówno w relacji bezpośrednio pomiędzy tymi czynami, jak i w zbiegu z przestępstwami innych rozdziałów części szczególnej Kodeksu karnego. Autor, posiłkując się w tym zakresie poglądami innych autorów, jak też przedstawiając własne oceny poszczególnych możliwych zbiegów przepisów i przestępstw, analizuje zachodzące w tym zakresie sytuacje, w tym także wskazuje, który w jego ocenie przepis znajdzie w danym wypadku zastosowanie.

W rozdziale szóstym pt. Uwagi prawnoporównawcze autor dokonuje natomiast omówienia regulacji z zakresu prawa karnego materialnego, bezpośrednio związanych z szeroko rozumianą problematyką przestępstw hackerskich, w tym przestępstw skierowanych przeciwko bezpieczeństwu informacji, systemów komputerowych i sieci informatycznych, a obowiązujących w wybranych krajach europejskich. Należy przy tym z dużym szacunkiem odnieść się do znacznego nakładu pracy autora związanej z prześledzeniem poszczególnych, zagranicznych regulacji karnoprawnych, a także przedstawieniem ich w skondensowanej, ale zarazem przejrzystej i dostępnej formie.

Ostatni rozdział – siódmy, ma charakter opracowania kryminologicznego oraz obejmuje analizę badań opartych na metodzie statystycznej oraz badań empirycznych, a dotyczących skali i rozmiaru przestępczości komputerowej (w tym także zjawiska hackingu) w Polsce. Autor poddaje ocenie statystyki policyjne i zauważa, że większość przestępstw popełnianiach głównie za pośrednictwem sieci Internet (ok. 80%) stanowią tzw. oszustwa internetowe, które co do zasady zazwyczaj realizują znamiona klasycznego

występku z art. 286 § 1 KK, oraz że można zaobserwować w Polsce zjawisko stałego wzrostu przestępstw stwierdzonych – popełnianych za pośrednictwem sieci Internet. Z uwagi także na zbiorczy sposób przedstawiania w statystykach policyjnych liczby wszczętych postępowań oraz przestępstw stwierdzonych, co przejawia się np. w łączeniu w jednej grupie występków z art. 267 § 1, z art. 267 § 2, z art. 267 § 3 i z art. 267 § 4 KK, bez wyróżnienia, ile z nich dotyczy faktycznie przestępstw komputerowych, a ile przestępstw pospolitych (np. „przeciwko korespondencji" lub związanych z „tradycyjnym" podsłuchem telefonu), jak słusznie zauważa autor, statystyki te są mało przydatne dla zobrazowania rzeczywistej skali przestępczości komputerowej, w tym także *stricte* hackerskiej w Polsce.

Autor przedstawia także w rozdziale siódmym wyniki własnych badań empirycznych, w zakresie analizy akt prokuratorskich spraw dotyczących przestępstw z art. 267 § 2, z art. 268 § 2 i 3, z art. 268a § 1 i 2, z art. 269 § 1 i 2, z art. 269a oraz z art. 269b § 1 KK, zarejestrowanych w powszechnych jednostkach organizacyjnych prokuratur w latach 2009–2010, w łącznej liczbie 1163 spraw. Dodatkowo autor prezentuje w zanonimizowanej formie wybrane stany faktyczne, dotyczące niektórych spraw prowadzonych uprzednio przez prokuratury. Przedstawione przykłady omawianych stanów faktycznych – opartych na konkretnych sprawach karnych – pozwalają prześledzić pewien *modus operandi* sprawców najpopularniejszych w polskich warunkach czynów, realizowanych za pośrednictwem sieci Internet.

Reasumując, monografię *F. Radoniewicza* pt. Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym uznać można za bardzo istotną na polskim rynku prawniczym i wartą polecenia publikację. Z oczywistych względów wymaga ona aktualnie nieznacznej korekty (głównie w zakresie dotyczącym rozdziału piątego), z uwagi na zmiany ustawodawcze, które weszły w życie już po publikacji, a dotyczące nowelizacji treści art. 269a, art. 269b § 1 KK, oraz dodania do rozdziału XXXIII nowych przepisów, tj. art. 269b § 1a oraz art. 269c KK.

Nie ulega również wątpliwości, że publikacja ta w szerokim zakresie spełni oczekiwania praktyków, w tym także sędziów i prokuratorów, w zakresie umożliwiającym im uzyskanie niezbędnej wiedzy specjalistycznej z dziedziny tzw. przestępczości hackerskiej.