dr Mikołaj Małecki
Bartosz Kwiatkowski

Opinia w sprawie odpowiedzialności karnej uczestnika programu *bug bounty* (na gruncie polskiego Kodeksu karnego)

Kraków, dnia 9 grudnia 2016 r.

1.

Przedmiotem opinii jest ocena prawna działalności osoby zajmującej się znajdowaniem błędów w systemach/sieciach teleinformatycznych lub informatycznych (dalej, dla uproszczenia, określenia te używane będą zamiennie) w celu zwrócenia uwagi ich właścicielowi, iż system bądź sieć posiada wady i luki. Z perspektywy poniższych rozważań wyróżnić można dwie podstawowe sytuacje, w których mamy do czynienia ze wskazaną działalnością:

1) program *bug bounty*, w ramach którego jest ona realizowana za zgodą, a nawet na zlecenie dysponenta systemu/sieci,
2) zachowania podejmowane z własnej inicjatywy testera, który ma zamiar poinformowania osoby uprawnionej o ewentualnie wykrytych błędach bądź lukach w działaniu systemu/sieci.

Analiza obowiązujących regulacji Kodeksu karnego prowadzi do wniosku, że wyszukiwanie błędów w systemach/sieciach teleinformatycznych lub informatycznych w obu wskazanych przypadkach **nie powinno być uznawane za realizację znamion czynu zabronionego pod groźbą kary**.

1.1. Zachowanie osoby zajmującej się wyszukiwaniem nieprawidłowości i luk działania systemu informatycznego nie godzi w dobro prawne właściciela systemu, jeśli podjęte jest w celu ochrony bezpieczeństwa danego systemu, tj. ujawnienia i przekazania informacji o stwierdzonych nieprawidłowościach osobie uprawnionej.

1.2. Dodatni społecznie cel działania osoby podejmującej omawiane zachowania zasadniczo w żadnym wypadku, także w razie działania z własnej inicjatywy testera, nie pozwala uznać, że osoba ta narusza normę postępowania mającą chronić system informatyczny przed zewnętrznymi atakami osób nieuprawnionych. Tym bardziej testowanie systemu informatycznego za zgodą administratora nie może naruszyć aktualizującej się w tym przypadku normy sankcjonowanej, gdyż zgoda dysponenta dobra upoważnia dany podmiot do podejmowania odpowiednich działań w zakresie udzielonej zgody.

1.3. Tylko zachowania cechujące się *in abstracto* odpowiednim stopniem karygodności mogą zostać zabronione pod groźbą kary w rozumieniu art. 1 § 1 k.k. Nie spełniają tego warunku działania zmierzające do polepszenia bezpieczeństwa danych informatycznych, polegające na podejmowaniu wskazanych zachowań na zlecenie lub za zgodą osoby uprawnionej, bądź też z własnej inicjatywy testera i w uczciwym celu.

1.4. Regulacje prawa międzynarodowego dają możliwość uwzględnienia, w procesie wykładni i stosowania polskiego prawa karnego, dodatniego społecznie celu działania osoby testującej system informatyczny.

1.5. Przystosowanie urządzeń, programów komputerowych lub haseł, o których mowa w art. 269b § 1 k.k., powinno być rozumiane w sposób subiektywny jako przystosowanie ich w celu popełnienia przestępstwa godzącego w bezpieczeństwo informacji.

1.6. Art. 269b § 1 k.k. wprowadza karalność klasycznych czynności przygotowawczych do przestępstwa, co sprawia, że mają do niego

zastosowanie wszystkie warunki odpowiedzialności karnej określone w art. 16 k.k. W szczególności, warunkiem bezprawności czynu jest towarzyszący sprawcy cel dokonania określonego przestępstwa rodzajowego, natomiast dobrowolne odstąpienie sprawcy od kontynuowania czynności przygotowawczych, w tym pozbycie się urządzeń i programów przystosowanych, zgodnie z zamiarem sprawcy, do dokonania przestępstwa, jest okolicznością wyłączającą karalność czynu, zgodnie z art. 17 § 1 k.k.

1.7. W aktualnym stanie prawnym stwierdzenie braku odpowiedzialności karnej osoby podejmującej opisane zachowania, w społecznie dodatnim celu, nie wymaga wprowadzania zmian w przepisach karnych.

1.8. W niniejszej opinii zagadnienie testowania systemu teleinformatycznego zostało przeanalizowane wyłącznie z perspektywy przepisów prawa karnego. Nie można wykluczyć odpowiedzialności osoby testującej system informatyczny – w szczególności gdy podejmuje ona swoje działania bez zgody osoby uprawnionej – na podstawie regulacji zawartych w innych gałęziach prawa, np. prawa cywilnego czy administracyjnego, jednak problematyka ta nie stała się przedmiotem poniższych rozważań.

2.

Zgodnie z tytułem rozdziału XXXIII Kodeksu karnego, zachowania opisane w przepisach zgrupowanych w tym rozdziale **mają godzić w bezpieczeństwo danych i informacji**, które jej dysponent chce objąć ochroną przed dostępem osób nieuprawnionych. Zachowanie osoby zajmującej się wyszukiwaniem nieprawidłowości i luk działania systemu informatycznego nie godzi w tak scharakteryzowane dobro prawne, jeśli podjęte jest w celu ochrony bezpieczeństwa danego systemu na przyszłość, a więc w zamiarze ujawnienia i przekazania informacji o stwierdzonych nieprawidłowościach osobie uprawnionej. Skoro zachowanie to, podjęte w określonym celu, służy ochronie informacji, to nie może stanowić jednocześnie ataku na dobro prawne w postaci bezpieczeństwa informacji, wymaganego dla uznania danego czynu za wyczerpanie znamion przedmiotowych

czynu zabronionego pod groźbą kary. Ustalenia te powinny rzutować na wykładnię wszystkich przepisów zgrupowanych w rozdziale XXXIII Kodeksu karnego.

Należy uznać, że uzyskanie dostępu do informacji w rozumieniu art. 267 § 1 k.k. lub uzyskanie dostępu do systemu informatycznego w rozumieniu art. 267 § 2 k.k. wyłącznie w celu stwierdzenia i przekazania informacji o ewentualnym błędzie lub luce w działaniu systemu informatycznego uprawnionemu podmiotowi (właścicielowi lub innemu dysponentowi systemu), jako zachowanie nie atakujące dobra prawnego, nie wyczerpuje znamion czynu zabronionego pod groźbą kary. Dotyczy to zarówno sytuacji, w której osoba dopuszczająca się opisanych działań czyni to w ramach programów *bug bounty*, tj. za zgodą osoby uprawnionej, jak również wypadków, w których działa z własnej inicjatywy.

W opisanych przypadkach tylko pozornie dochodzi do abstrakcyjnego zagrożenia dla dobra prawnego, jakim jest bezpieczeństwo danych, na co wskazuje pozytywny w ocenie społecznej, służący ochronie dóbr prawnych osoby uprawnionej, cel działania danego podmiotu. Sytuację tę można porównać do wejścia w posiadanie kluczy do mieszkania innej osoby – która pozostawiła te klucze bez nadzoru w miejscu publicznym – w celu oddania ich osobie uprawnionej i dodatkowo zwrócenia jej uwagi na niebezpieczeństwo wynikające z ich pozostawienia bez należytej opieki. Zachowanie to zagraża własności jedynie pozornie (ktoś, kto wszedł w posiadanie kluczy do mieszkania, może dostać się do niego i coś ukraść) – pozytywny cel działania podmiotu sprawia, że jego postępowanie jest społecznie opłacalne (zwrot kluczy ich właścicielowi).

3.

Opisywane działania są podejmowane w celu ochrony danego systemu informatycznego, a więc nie zmierzają do naruszenia dobra prawnego, co sprawia, że w aspekcie aksjologicznym normy sankcjonowanej, leżącej u podstaw opisanych przestępstw, **zachowania te nie są zachowaniami niedozwolonymi** (a przynajmniej nie można ich uznać za zachowania

relewantne prawnokarnie, jeśliby stanowiły naruszenie norm administracyjnych czy cywilnoprawnych). Warto zaznaczyć, że analiza normatywna przepisów prawa karnego jest już współcześnie powszechnie przyjętą, a zapoczątkowaną jeszcze w latach 90. XX wieku metodą interpretacyjną, służącą do uadekwatnienia i racjonalizowania przepisów obowiązującego prawa. W powiązaniu z powszechnie przyjmowaną w doktrynie prawa karnego nauką o tzw. strukturze przestępstwa, analiza normatywna jest nieodzownym punktem odniesienia przy interpretacji Kodeksu karnego, pozwalającym unikać pozornych problemów i rzekomych paradoksów. Każda norma postępowania w systemie państwa prawa ustanawiana jest po coś; norma prawna ma czemuś służyć i tylko zachowania wpisujące się w przewidziany przez ustawodawcę cel ochronny normy mogą być uznane za czyny bezprawne (na temat analizy normatywnej szerzej zob. A. Zoll, *Karalność i karygodność czynu jako odrębne elementy struktury przestępstwa*, w: *Teoretyczne problemy odpowiedzialności karnej w polskim oraz niemieckim prawie karnym*, red. T. Kaczmarek, Wrocław 1990, s. 101 i n.; K. Buchała, A. Zoll, *Polskie prawo karne*, Warszawa 1997, s. 71 i n.; Ł. Pohl, *Struktura normy sankcjonowanej w prawie karnym. Zagadnienia ogólne*, Poznań 2007, s. 27 i n.; *J. Majewski, Budowa przepisów prawa karnego i norm w nich zawartych*, w: *System Prawa Karnego*, t. 2, red. T. Bojarski, Warszawa 2011, s. 459 i n.; M. Dąbrowska-Kardas, *Analiza dyrektywalna przepisów części ogólnej kodeksu karnego*, Warszawa 2012, s. 133 i n.; P. Kardas, *O relacjach między strukturą przestępstwa a dekodowanymi z przepisów prawa karnego strukturami normatywnymi,* „Czasopismo Prawa Karnego i Nauk Penalnych" 2012, nr 4, s. 5 i n.; W. Wróbel, A. Zoll, *Polskie prawo karne. Część ogólna*, Kraków 2012, s. 107; Ł. Pohl, *Prawo karne. Wykład części ogólnej*, Warszawa 2013, s. 48 i n.).

Norma sankcjonowana wiążąca określone osoby w omawianej kategorii przypadków ma na celu odpowiednie zabezpieczenie informacji, które dysponent danych zgromadził w przestrzeni wirtualnej. Testowanie systemu informatycznego za zgodą administratora nie może naruszyć interesującej nas w tym przypadku normy sankcjonowanej, gdyż **zgoda dysponenta dobra upoważnia dany podmiot do podejmowania**

odpowiednich działań w zakresie udzielonej zgody. Należy podkreślić, że zgoda dysponenta dobra nie jest tzw. kontratypem, czyli okolicznością uchylającą bezprawność czynu dopiero po stwierdzeniu realizacji znamion czynu zabronionego, lecz jest okolicznością uprawniającą daną osobę do podjęcia zachowania *ex ante* legalnego, nie wymagającego usprawiedliwienia z odwołaniem się do instytucji kontratypu (przykładowo, zniszczenie rzeczy za zgodą jej właściciela jest zachowaniem prawnie dozwolonym; nie ma potrzeby odwoływania się w tym zakresie do instytucji kontratypu).

Z uwagi na specyfikę analizowanych sytuacji faktycznych, mieszczących się na dalekim przedpolu zagrożenia dla dobra prawnego, dodatni społecznie cel działania osoby podejmującej opisywane zachowania zasadniczo w żadnym wypadku, także w razie działania z własnej inicjatywy testera, nie pozwala uznać, że osoba ta narusza normę postępowania mającą na celu ochronę informacji przed zewnętrznymi atakami osób nieuprawnionych. W analizowanym obszarze aktywności społecznej zostają wypracowane, w praktyce życia, **reguły ostrożności wiążące użytkowników sieci**. Przekonanie o społecznej opłacalności i dozwolonym charakterze opisywanych działań umacnia ponadto praktyka wynagradzania pracy indywidualnych testerów, zgłaszających wykrycie luki bądź błędów w działaniu danego systemu, pojawiająca się nierzadko *ex post* z inicjatywy samych administratorów czy właścicieli systemów teleinformatycznych, którzy – w dobrze pojmowanej trosce o swój własny interes – są *de facto* „wdzięczni" testerowi za wykonaną pracę. W rezultacie należy stwierdzić, że wychwycenie i wskazanie luk w systemie informatycznym mającym zabezpieczyć pewnego rodzaju informacje, służy polepszeniu ich ochrony, a przez to w państwie prawa, będącym dobrem wspólnym wszystkich obywateli, jawi się jako zachowanie nie tylko dozwolone, ale wręcz nakazane, społecznie korzystne i zasługujące na aprobatę.

4.

Zasadność odwoływania się do celu działania osoby testującej system teleinformatyczny znajduje potwierdzenie w przepisach Kodeksu karnego.

Należy podkreślić, że zachowanie całkowicie pozbawione cechy społecznej szkodliwości nie jest nawet w minimalnym stopniu karygodne (art. 1 § 2 k.k.), a więc w kontekście wieloaspektowej struktury przestępstwa zachowanie to nie wyczerpuje w ogóle znamion czynu zabronionego pod groźbą kary (art. 1 § 1 k.k.). **Tylko zachowanie cechujące się *in abstracto* odpowiednim stopniem karygodności może być zachowaniem zasługującym na karę kryminalną w rozumieniu art. 1 k.k.** Zob. A. Zoll, w: *Kodeks karny. Część ogólna. Tom I. Część I. Komentarz do art. 1-52*, red. W. Wróbel, A. Zoll, Warszawa 2016, komentarz do art. 1 k.k., który zaznacza: „Z zasad konstytucyjnych (przede wszystkim z zasady demokratycznego państwa prawnego i wynikającej z niej zasady stosunkowości) wynika, że ustawodawcy nie wolno zakazywać pod groźbą kary zachowań, które nie godzą w dobra mające społeczną wartość, a tym bardziej zachowań, które stanowią realizację podstawowych wolności i praw jednostki gwarantowanych Konstytucją" (teza 3), a także: „Czyn, który jest pozbawiony cechy społecznej szkodliwości, nie może być zakwalifikowany jako czyn zabroniony" (teza 6). Również A. Wąsek stwierdza, że: „jeżeli [...] okaże się, że dany czyn w ogóle nie naraża dobra prawnokarnie chronionego, to wówczas należy uznać, że nie zawiera on znamion czynu zabronionego (art. 17 § 1 pkt 2 k.p.k.)" (A. Wąsek, *Kodeks karny. Komentarz. Tom I. (art. 1-31),* Gdańsk 1999, s. 30).

De lege lata motywacja sprawcy i postać zamiaru (w tym treść zamiaru) wpływają na ocenę stopnia społecznej szkodliwości czynu, zgodnie z art. 115 § 2 k.k. Co oczywiste, ze względu na negatywną motywację sprawcy, karalne pozostaje zachowanie polegające na przełamaniu zabezpieczenia danego systemu informatycznego i zażądaniu wynagrodzenia za usunięcie luki pod groźbą upublicznienia wykrytych nieprawidłowości. Jeżeli jednak społeczna szkodliwość czynu równa jest zeru bądź przedstawia wartość ujemną (a więc czyn jest społecznie opłacalny), *ex ante* nie stanowi on przestępstwa. Również w ten sposób łatwo dojść do wniosku, że zachowania będące przedmiotem niniejszej opinii, jako obiektywnie społecznie opłacalne i subiektywnie niezagrażające dobru prawnemu, nie mogą stanowić podstawy odpowiedzialności karnej.

Zobowiązania międzynarodowe wymagają od Rzeczypospolitej Polskiej kryminalizacji zachowań polegających m.in. na umyślnym, bezprawnym dostępie do całości lub części systemu informatycznego. W literaturze celnie podkreśla się jednak, że „strony mogą ograniczyć karalność omawianego czynu [tj. czynu z art. 267 k.k. – dop. nasz, B.K., M.M.], wprowadzając wymóg, że do jego popełnienia wymagane jest naruszenie zabezpieczeń lub konieczność wystąpienia po stronie sprawcy zamiaru kierunkowego – **działania w celu pozyskania danych komputerowych lub z innym nieuczciwym zamiarem**" (F. Radoniewicz, *Uzyskanie bezprawnego dostępu do systemu komputerowego*, w: *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, podrozdział 3.3.2.3). Wynika to wprost z art. 2 konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. 2015, poz. 728): „Strona może wprowadzić wymóg, że przestępstwo musi zostać popełnione poprzez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym". Regulacje te dają możliwość uwzględnienia w procesie wykładni i stosowania prawa dodatniego społecznie celu działania osoby odpowiedzialnej za testowanie systemu teleinformatycznego.

5.

Szczególne kontrowersje wywołuje treść art. 269b § 1 k.k., zgodnie z którym: „Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3".

Nietrudno zauważyć, że powierzchowna wykładnia wskazanego przepisu prowadzi do nieracjonalnego rozszerzenia zakresu kryminalizacji na

zwykłe czynności dnia codziennego, podejmowane przez większość członków społeczeństwa. Każdy posiadacz komputera czy smartfonu jest bowiem w posiadaniu urządzenia obiektywnie przystosowanego do popełnienia przestępstw przeciwko bezpieczeństwu informacji (standardowy system operacyjny komputera jest przystosowany do zalogowania się na konto pocztowe innej osoby i kradzieży znajdujących się tam wiadomości, nawet jeśli jego właściciel nie ma zamiaru tego czynić). Oznacza to, że ekstensywna wykładnia omawianej regulacji powinna zostać odrzucona jako niekoherentna systemowo i sprzeczna z *ratio legis* przestępstwa opisanego w art. 269b k.k.

Przede wszystkim nie wyczerpują znamion czynu zabronionego z art. 269b § 1 k.k. czynności podjęte **za zgodą podmiotu uprawnionego**, który swobodnie dysponuje swym dobrem prawnym, wskutek czego podejmowanie analizowanych tu czynności staje się działaniem legalnym. W tym zakresie pominięcie w art. 269b § 1 k.k. znamienia „wbrew uprawnieniom" (lub analogicznego, wskazującego na wymóg bezprawności czynu) jest jedynie pozorne. Zob. w tym samym kierunku W. Wróbel, w: *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k.*, red. A. Zoll, Warszawa 2013, komentarz do art. 269b k.k., teza 6: „Z uwagi na tytuł rozdziału XXXIII, wskazujący na rodzajowy przedmiot ochrony, zachowania opisane w art. 269b podlegają karze tylko wówczas, gdy podejmowane są przez osobę nieuprawnioną. Pominięcie tej klauzuli w treści art. 269b należy uznać za przeoczenie ustawodawcy".

Równie istotna okazuje się właściwa interpretacja znamienia „przystosowane". Należy uznać, że przystosowanie urządzeń lub programów komputerowych, o którym mowa w tym przepisie, powinno być rozumiane w sposób **subiektywny** jako przystosowanie ich w specyficzny sposób **w celu popełnienia jednego lub wielu przestępstw atakujących bezpieczeństwo informacji**. Również w zakresie haseł komputerowych, kodów dostępu i innych danych umożliwiających dostęp do informacji (art. 269b § 1 *in fine* k.k.) wymagane musi być **celowe działanie sprawcy ukierunkowane na popełnienie konkretnego przestępstwa przeciwko**

ochronie informacji. Trafnie zauważa się w literaturze karnistycznej, że mamy tu do czynienia z zakamuflowanym typem przygotowania do przestępstwa, tj. przepisem penalizującym **czynności przygotowawcze w rozumieniu art. 16 § 2 k.k.** (zob. zgodnie w tej kwestii: W. Wróbel, w: *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k.*, red. A. Zoll, Warszawa 2013, komentarz do art. 269b k.k., teza 3; P. Kozłowska-Kalisz, w: *Kodeks karny. Komentarz*, red. M. Mozgawa, Warszawa 2016, komentarz do art. 269b k.k., teza 2; J. Giezek, w: *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2014, komentarz do art. 269b k.k., teza 2; A. Sakowicz, w: *Kodeks karny. Część szczególna. Tom II. Komentarz do artykułów 222–316*, red. M. Królikowski, R. Zawłocki, Warszawa 2013, komentarz do art. 269b k.k., teza 1; B. Kunicka-Michalska, w: *Kodeks karny. Część szczególna. Komentarz do artykułów 222–316. Tom II*, red. A. Wąsek, R.Zawłocki, Warszawa 2010, komentarz do art. 269b k.k., tezy 4 i 5; K. Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b Kodeksu karnego*, „Prokurator" 2005, nr 1, s. 75).

W tym kontekście S. Hoc stwierdza wprost: „Przepis art. 269b § 1 k.k. dotyczy tylko takich urządzeń lub programów, które celowo zostały przystosowane do popełnienia wymienionych w nim przestępstw. Powyższa interpretacja ma swoje granice w definicji karalnych czynności przygotowawczych z art. 16 § 1 k.k. W przeciwnym przypadku zakres karalności przewidziany w tym przepisie znacznie wykraczałby poza racje kryminalno-polityczne leżące u podstaw jego wprowadzenia do k.k." (S. Hoc, w: *Kodeks karny. Komentarz*, red. R.A. Stefański, Legalis 2016, wydanie elektroniczne, komentarz do art. 269b k.k., teza 8). Również K. Gienas zauważa: „Wydaje się, że co do zasady, rozstrzygającym kryterium dla oceny czy mamy do czynienia z narzędziem hackerskim powinien być **zamiar** towarzyszący producentowi oprogramowania" (K. Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b Kodeksu karnego*, „Prokurator" 2005, nr 1, s. 78).

W praktyce poglądy te uzyskały poparcie przedstawicieli organów ścigania (zob. B. Długołęcka, Biuro Spraw Konstytucyjnych, Prokuratura Generalna,

pismo z dn. 19 września 2013 r., s. 3-4, ze zwróceniem uwagi na konstytutywny dla omawianego przestępstwa, celowy charakter podejmowanych czynności, https://niebezpiecznik.pl/hacking-prokuratura.pdf).

Przytoczone, jednolite poglądy doktryny prawa karnego wskazujące na wymóg bezprawnego celu działania sprawcy, charakterystycznego dla formy stadialnej przygotowania, prowadzą do jednoznacznego wniosku, iż nie jest dopuszczalne potraktowanie jako przestępstwa działania osoby, która z własnej inicjatywy zajmuje się wyszukiwaniem luk w działaniu systemów informatycznych w *ex ante* uczciwym celu poinformowania o stwierdzonych nieprawidłowościach właściciela systemu.

6.

Do czynności opisanych w art. 269b § 1 k.k. znajdują zastosowanie ogólne warunki odpowiedzialności za przygotowanie do przestępstwa, zdefiniowane w art. 16 § 1 *in principio* k.k. Zgodnie z tym przepisem, warunkiem odpowiedzialności za przygotowanie do przestępstwa jest **cel dokonania określonego przestępstwa rodzajowego**, towarzyszący sprawcy w czasie podejmowania czynności przygotowawczych (np. cel włamania się do systemu informatycznego po to, aby wykraść dane i dokonać ich odsprzedaży). Sprawca przygotowania ma podejmować czynności mające stworzyć mu warunki do przedsięwzięcia dalej idących czynów, ukierunkowanych na naruszenie dobra prawnego, tj. ma podejmować je dlatego, że **chce osiągnąć za ich sprawą bezprawny rezultat** w postaci dokonania określonego przestępstwa rodzajowego.

W analizowanym przepisie nie jest zatem przewidziana karalność samego w sobie abstrakcyjnego zagrożenia dla dobra prawnego, lecz kryminalizacji podlega zagrożenie związane ze ściśle określonym, nagannym społecznie celem działania sprawcy. W przypadku klasycznego przygotowania do przestępstwa negatywny stosunek mentalny sprawcy do czynu jest determinantą bezprawności czynu (bez ustalenia celu działania ukierunkowanego na naruszenie dobra prawnego, określone czynności nie mogą być uznane za czyny bezprawne).

Działania mające na celu zidentyfikowanie i przekazanie podmiotowi uprawnionemu informacji o nieprawidłowościach i lukach w systemie informatycznym, z użyciem standardowego, nie odbiegającego od stosowanego w praktyce życia w tej profesji oprogramowania czy innych urządzeń wykorzystywanych przez informatyków, a także działania przygotowawcze zmierzające do osiągnięcia tego korzystnego społeczne celu nie wyczerpują znamion przestępstwa opisanego w art. 269b k.k. w kontekście obligatoryjnych znamion przygotowania do przestępstwa określonych w art. 16 § 1 k.k.

7.

Wnioski płynące z przeprowadzonych rozważań wzmacnia odwołanie się do reguł wykładni prokonstytucyjnej i prokonwencyjnej. Należy zaznaczyć, że uwzględnianie szeroko rozumianych uwarunkowań systemowych w ramach analiz wykładniczych na gruncie przepisów prawa karnego, w tym aktów prawnych wyższego rzędu oraz regulacji prawa międzynarodowego, a także poszukiwanie takiego rezultatu wykładni, który zagwarantuje realizację w danym porządku prawnym wartości konstytucyjnych (zgodność analizowanego przepisu z wzorcem konstytucyjnym i konwencyjnym), jest współcześnie szeroko akceptowaną metodą interpretacji (zob.: K. Szczucki, *Wykładnia prokonstytucyjna prawa karnego,* Warszawa 2015; P. Skalimowski, *Granice między wykładnią prokonstytucyjną a bezpośrednim stosowaniem przepisów Konstytucji – uwagi na tle uchwały Izby Gospodarczej NSA z 22 czerwca 2011 r.*, „Palestra" 2013, nr 3-4, s. 299 i n., T. Grzybowski, *Wpływ zmian prawa na jego wykładnię*, Warszawa 2013, a także orzecznictwo, w którym odwołano się do metod wykładni prokonstytucyjnej, np. wyrok Sądu Najwyższego z dnia 17 października 2012 r., IV KK 99/12, LEX nr 1231601; Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 1 czerwca 2012 r., II FSK 2420/10, LEX nr 1215541). W przypadku konkurowania ze sobą kilku hipotez interpretacyjnych, prymat należy przyznać wykładni zgodnej (najbardziej zgodnej) ze standardem konstytucyjnym i wspólnotowym („Wykładnia prowspólnotowa i inne kanony wykładni pozajęzykowej nie mogą więc popaść w konflikt; w tym sensie wykładnia prokonstytucyjna ma pierw-

szeństwo przed innymi kanonami wykładni" – zob. T. Spyra, *Granice wykładni prawa. Znaczenie językowe tekstu prawnego jako granice wykładni*, Warszawa 2006).

W aspekcie systemowo-konstytucyjnym ograniczenie zakresu zastosowania omawianych przepisów przez uwzględnienie dodatniego społecznie celu działania sprawcy, ewaluującego daną kategorię zachowań jako czynów niezasługujących na negatywną ocenę społeczną, zapewnia zgodność omawianych regulacji Kodeksu karnego z art. 31 ust. 3 Konstytucji RP (**wymóg proporcjonalności** – w tym konieczności – ograniczenia praw i wolności człowieka) i art. 42 ust. 1 Konstytucji RP (**wymóg dostatecznej określoności** znamion zachowania karalnego w aspekcie zewnętrznym i wewnętrznym). Odmienna interpretacja opisanych przepisów prowadziłaby do naruszenia standardu konstytucyjnego przynajmniej we wskazanym wyżej zakresie; przepisy te przestałyby trafiać w swój ustawowy cel, jakim jest zapewnienie ochrony danych zgromadzonych w systemie informatycznym.

W aspekcie systemowo-konwencyjnym pierwszorzędne znaczenie dla prawidłowej wykładni omawianych przepisów ma art. 6 konwencji Rady Europy o cyberprzestępczości, zgodnie z którym: „1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, **umyślnych i bezprawnych**: a. produkcji, sprzedaży, pozyskiwania **z zamiarem** wykorzystania, importowania, dystrybucji lub innego udostępniania: i. urządzenia, w tym także programu komputerowego, **przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw** określonych zgodnie z artykułami 2-5; ii. hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna, **z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw** określonych zgodnie z artykułami 2-5; oraz b. posiadania elementu wymienionej powyżej w punktach a. i. lub ii. **z zamiarem wykorzystania w celu popełnienia któregokolwiek z przestępstw** określonych zgodnie

z artykułami 2-5. Strona może w swoim prawie wprowadzić wymóg, że odpowiedzialność karna dotyczy posiadania większej ilości takich jednostek. 2. Niniejszego artykułu nie należy interpretować jako mającego na celu pociągnięcie do odpowiedzialności karnej w przypadku, kiedy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie, o którym mowa w ustępie 1 niniejszego artykułu, **nie jest dokonywane w celu popełnienia przestępstwa określonego zgodnie z artykułami 2-5 niniejszej konwencji, jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego**".

Wskazane przepisy, będące historycznym i prawnym tłem wprowadzenia do polskiego Kodeksu karnego art. 269b, jednoznacznie wskazują na wymóg podjęcia określonych zachowań sprawczych „w celu" popełnienia określonego przestępstwa, a więc mamy tu do czynienia w istocie rzeczy z ograniczeniem zakresu kryminalizacji do typowych czynności przygotowawczych, scharakteryzowanych w art. 16 § 1 k.k. (czynności celowe znamienne zamiarem bezpośrednim). Tak również trafnie podkreśla się w literaturze: „[...] w art. 6 Konwencji o cyberprzestępczości przewiduje się zastrzeżenia mające na celu ograniczyć zakres kryminalizacji. Dla bytu tego przestępstwa, zgodnie z Konwencją o cyberprzestępczości, musi być spełniony – po pierwsze – wymóg, by sprawca miał zamiar, by narzędzie zostało użyte do popełnienia przestępstwa określonego w art. 2–5, a więc by działał w zamiarze kierunkowym. Po drugie, urządzenia i programy komputerowe **muszą być zaprojektowane lub przystosowane głównie (ang. *primarily*) do popełnienia któregoś z przestępstw** określonych w Konwencji o cyberprzestępczości (oba te rozwiązania przyjmuje dyrektywa 2013/40 dotycząca ataków na systemy informatyczne)" (F. Radoniewicz, *Artykuł 269b k.k. – tzw. bezprawne wykorzystanie urządzeń, programów i danych*, w: *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, podrozdział 5.10, Warszawa 2016).

W identycznym kierunku zmierzają postanowienia Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW (Dz.U.UE L z dn. 14 sierpnia 2013 r.): „Państwa członkowskie podejmują środki niezbędne do zagwarantowania, by umyślne wytwarzanie, sprzedaż, dostarczanie w celu użycia, przywóz, rozpowszechnianie lub udostępnianie w inny sposób jednego z następujących narzędzi było karalne jako przestępstwo, **jeżeli zostało dokonane bezprawnie i umyślnie w celu popełnienia któregokolwiek z przestępstw**, o których mowa w art. 3-6, co najmniej w przypadkach, które nie są przypadkami mniejszej wagi: a) programu komputerowego, zaprojektowanego lub przystosowanego głównie do celu popełniania przestępstw, o których mowa w art. 3-6; b) hasła komputerowego, kodu dostępu lub podobnych danych umożliwiających dostęp do całości lub części systemu informatycznego".

Na konieczność dostosowania polskich regulacji prawnych do wymogów Konwencji Rady Europy o cyberprzestępczości zwracano uwagę w uzasadnieniu wprowadzenia do Kodeksu karnego art. 269b k.k., pisząc: „Zmiany w art. 268 § 2 k.k. oraz nowe regulacje proponowane w art. 269a k.k. i art. 269b K.k. mają swoje źródło w przepisach Konwencji o cyberprzestępczości [...]. Artykuł 6 Konwencji zawiera przepisy zobowiązujące strony do spenalizowania produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania, a także posiadania z zamiarem wykorzystania narzędzi i programów hakerskich oraz haseł i kodów dostępu. Penalizacja jest ograniczona do działań, których celem jest popełnienie jednego z przestępstw określonych w artykułach od 2 do 5 Konwencji. Artykuł ten przewiduje możliwość złożenia zastrzeżenia i ograniczenia przez Strony zakresu penalizacji do produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania haseł komputerowych, kodów dostępu lub podobnych danych, dzięki którym jest możliwe uzyskanie dostępu do całości lub części systemu komputerowego" (zob. rządowy projekt ustawy o zmianie ustawy – Kodeks karny, ustawy –

Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń, druk nr 2031, Sejm IV kadencji, http://orka.sejm.gov.pl/Druki4ka.nsf/wgdruku/2031; http://orka.sejm.gov.pl/proc4.nsf/0/4FBF6FEB0B1B1CD2C12570C700300717?OpenDocument).

8.

Uznanie typu czynu zabronionego za przejaw kryminalizacji przygotowania do przestępstwa wyklucza możliwość objęcia odpowiedzialnością karną etapu usiłowania tego typu czynu. Nie jest możliwe usiłowanie przygotowania, gdyż usiłowanie, zgodnie z art. 13 § 1 k.k., ma polegać na bezpośrednim zmierzaniu do „dokonania" czynu zabronionego. Nie ulega wątpliwości, że w omawianym kontekście jurydycznym, w przepisie traktującym o jednej z form stadialnych przestępstwa, ustawodawca pisząc o zmierzaniu do „dokonania" miał na myśli wyłącznie dokonanie; co oczywiste, ani usiłowanie nie jest dokonaniem, ani przygotowanie nie jest dokonaniem w rozumieniu tego przepisu. Wynika stąd, że tzw. usiłowanie przygotowania nie może wyczerpać znamion formy stadialnej opisanej w art. 13 § 1 k.k. (zob. M. Małecki, *Przygotowanie do przestępstwa. Analiza dogmatycznoprawna*, Warszawa 2016, s. 296; podrozdział 4.2.).

Należy uznać, że czyn opisany w art. 269b § 1 k.k. jest przestępstwem nieusiłowalnym, tzn. nie jest karalne usiłowanie jego popełnienia. Dolną granicą kryminalizacji czynów stypizowanych w art. 269b § 1 k.k. jest skuteczne wyczerpanie jednej z opisanych w tym przepisie czynności sprawczych oraz podjęcie jej w celu dokonania innego, ściśle określonego przestępstwa przeciwko bezpieczeństwu informacji.

Mimo realizacji znamion czynu zabronionego opisanego w art. 269b k.k., sprawca może uwolnić się od odpowiedzialności karnej, spełniając warunki czynnego żalu opisane w art. 17 § 1 k.k. Jest to prosta konsekwencja uznania omawianego przestępstwa za przejaw kryminalizacji czynności przygotowawczej. **Dobrowolne odstąpienie sprawcy od kontynuowania czynności przygotowawczych, w tym pozbycie się urządzeń i programów przystosowanych, zgodnie z zamiarem sprawcy, do**

dokonania przestępstwa, jest okolicznością wyłączającą karalność czynu: „Nie podlega karze za przygotowanie, kto dobrowolnie od niego odstąpił, w szczególności zniszczył przygotowane środki lub zapobiegł skorzystaniu z nich w przyszłości; w razie wejścia w porozumienie z inną osobą w celu popełnienia czynu zabronionego, nie podlega karze ten, kto nadto podjął istotne starania zmierzające do zapobieżenia dokonaniu" (art. 17 § 1 k.k.). W razie ziszczenia się przesłanek opisanych w tym przepisie, karalność czynu ustaje z mocy prawa i uwzględnienie tego faktu pozostaje poza zakresem dyskrecjonalnej władzy sędziego. Zob. wyrok Sądu Apelacyjnego w Białymstoku z dn. 20 czerwca 2006 r., II AKa 12/06, KZS 2007, z. 6, poz. 52: „Dobrowolne odstąpienie od przygotowania powoduje [...] wyłącznie karalności, a nie odstąpienie od wymierzenia kary. Odstąpienie od wymierzenia kary jest bowiem instytucją sądowego wymiaru kary i następuje w wyroku skazującym (art. 413 § 2 k.p.k.). Oznacza to, że sąd przypisuje sprawcy zarzucane przestępstwo, a jedynie odstępuje od orzeczenia kary. Różni to zasadniczo omawianą instytucję od ustawowej klauzuli niekaralności związanej z czynnym żalem z art. 17 k.k., która powoduje uchylenie karalności z mocy prawa, a w konsekwencji skutkuje umorzeniem postępowania lub wydaniem wyroku uniewinniającego (art. 17 § 1 pkt 4 oraz art. 414 § 1 k.p.k.)".

Do opisanej sytuacji faktycznej nie mają zastosowania regulacje czynnego żalu z art. 15 k.k., gdyż w fazie realizacji znamion czynu opisanego w art. 269b k.k., będącego wcześniejszą od usiłowania formą stadialną przestępstwa, nie dochodzi jeszcze do bezpośredniego zmierzania do dokonania określonego przestępstwa rodzajowego. Właściwym punktem odniesienia są więc warunki niekaralności określone w art. 17 k.k. Warto podkreślić, że przepis ten, względem sprawcy realizującego znamiona czynu zabronionego z art. 269b § 1 k.k., może zostać zastosowany wprost, a nie tylko na zasadzie analogii na korzyść sprawcy, choć procesowe konsekwencje zastosowania omawianej regulacji w sposób analogiczny byłyby w obu wypadkach identyczne (zob. W. Wróbel, w: *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k.*, red. A. Zoll, Warszawa 2013, komentarz do art. 269b k.k., teza 15: „W zakre-

sie, w jakim art. 269b przewiduje w istocie karalność za czynności przygotowawcze do popełnienia przestępstw z art. 165 § 1 pkt 4, art. 267 § 2, art. 268a § 1 albo § 2 w zw. z § 1, art. 269 § 2 albo art. 269a, możliwe jest na zasadzie dopuszczalnej analogii na korzyść sprawcy stosowanie art. 17, przewidującego instytucję czynnego żalu wyłączającego karalność", aprobująco wobec tego twierdzenia: S. Hoc, w: *Kodeks karny. Komentarz*, red. R.A. Stefański, Legalis 2016, wydanie elektroniczne, komentarz do art. 269b k.k., teza 14).

9.

W aktualnym stanie prawnym **stwierdzenie braku odpowiedzialności karnej osoby testującej w opisany wyżej sposób systemy informatyczne, w społecznie dodatnim celu, nie wymaga wprowadzania zmian w przepisach karnych**.

Ewentualne doprecyzowanie art. 269b § 1 k.k. w drodze inicjatywy legislacyjnej mogłoby zmierzać do odzwierciedlenia w warstwie językowej przepisu jego rzeczywistej zawartości normatywnej (nie byłaby to więc zmiana normatywna, lecz wzbogacenie przepisu o treści wynikające z jego kompleksowej interpretacji). Rozważyć można wprowadzenie do przepisu wyraźnej klauzuli wskazującej na wymóg celowego podjęcia określonych czynności mających stworzyć warunki do popełnienia określonych przestępstw wymierzonych w bezpieczeństwo informacji, np.: „Kto **w celu popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a**, wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane [*vel.* przeznaczone] do popełnienia takiego przestępstwa, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3".

Tego typu klauzula, wprowadzająca wymóg działania sprawcy z zamiarem bezpośrednim i kierunkowym, nie pozostawiałaby wątpliwości, że działa-

nia podejmowane na urządzeniach lub programach komputerowych, albo hasłach, kodach dostępu i innych danych umożliwiających dostęp do informacji stanowią karalne czynności przygotowawcze polegające na uzyskiwaniu środka przeznaczonego, w zamiarze sprawcy, do popełnienia przestępstwa (art. 16 § 1 k.k.). W tym zakresie przepis w zaproponowanym kształcie czyniłby zadość omówionym wyżej wymaganiom konwencyjnym i konstytucyjnym (w podobnym kierunku zmierzał nieuchwalony projekt nowelizacji art. 269b k.k. z dn. 1 grudnia 2010 r., zob. http://radalegislacyjna.gov.pl/sites/default/files/dokumenty/projekt_ustawy_1.pdf, w którym proponowano posłużyć się określeniem „przeznaczone" zamiast „przystosowane").

10.

W rezultacie przeprowadzonej analizy negatywnie należy ocenić koncepcje zmierzające do wyłączenia odpowiedzialności karnej za zachowania polegające na testowaniu bezpieczeństwa systemów informatycznych, tak za zgodą ich dysponentów, jak i z własnej inicjatywy, przez aplikację na grunt ustawy karnej instytucji kontratypu działalności naukowej czy swoistego kontratypu społecznej opłacalności danego rodzaju czynności. Podkreślić należy, iż testowanie systemu za zgodą właściciela jest zachowaniem od początku legalnym i niemogącym naruszyć interesów osoby uprawnionej, która przez fakt wyrażonej zgody potwierdza dopuszczalność podjęcia określonego zachowania, a wobec tego podmiot działający w ramach programu *bug bounty* nie wyczerpuje znamion czynu zabronionego z art. 269b § 1 k.k. czy nawet art. 267 § 1, 2 i 3 k.k. Nie jest również zachowaniem karalnym testowanie systemu przez daną osobę z jej własnej inicjatywy, w uczciwym, niebezprawnym celu (np. osoba prowadząca badania naukowe lub czynności śledcze polegające na uzyskiwaniu dostępu do systemu komputerowego). Wprowadzenie do treści przepisu klauzuli wskazującej jednoznacznie na cel działania sprawcy w wystarczającym stopniu ograniczyłoby zakres odpowiedzialności karnej za omawiane zachowania; do podobnych rezultatów dojść można także w aktualnym stanie prawnym, w drodze kompleksowej interpretacji przepisów obowiązującego prawa.

Konstrukcja swoistego kontratypu towarzysząca danemu przepisowi potwierdza, iż opisana w nim kategoria czynności wyczerpuje znamiona czynu zabronionego (w tym atakuje dobro prawne i narusza normę sankcjonowaną), sprawca nie popełnia jednak przestępstwa dopiero z uwagi na kolizję dóbr prawnych zachodzącą w danych okolicznościach oraz zamiar ocalenia dobra prawnego. W omawianych przypadkach sytuacja taka nie zachodzi. Jak wykazano, analizowana kategoria zachowań nie spełnia minimalnych warunków uznania ich za czyn karalny, tj. wymogu zagrożenia dobru prawnemu, warunku naruszenia normy sankcjonowanej i przesłanki społecznej szkodliwości czynu. Z tego powodu podjęcie opisywanych czynności nie aktualizuje norm sankcjonujących przewidzianych w polskim prawie karnym.