**KOMISJA KODYFIKACYJNA**

**PRAWA KARNEGO**

**Opinia w sprawie propozycji zmiany art. 269b § 1 Kodeksu karnego w związku z zarzutami Komisji Europejskiej dot. niepełnej transpozycji artykułu 7 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 (dalej: dyrektywa 2013/40)**

1. Projekt zakłada zamianę w treści art. 269b § 1 k.k. *De lege lata* typizuje on czyn polegający na wytwarzaniu, pozyskiwaniu, zbywaniu lub udostępnianiu innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w zw. z § 1, art. 269 § 2 albo art. 269a Kodeksu karnego, a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej. Stanowi zatem przejaw kryminalizacji zachowań leżących na przedpolu wymienionych w nim czynów zabronionych[[1]](#footnote-1).

Z uwagi na zastrzeżenia Komisji Europejskiej, wskazujące, że Polska nie dokonała pełnej transpozycji artykułu 7 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 (dalej: dyrektywa 2013/40)[[2]](#footnote-2) w zakresie penalizacji przestępstw, o których mowa w art. 3 i 6 dyrektywy 2013/40, projektowana zmiana polega na umieszczeniu w art. 269b § 1 k.k. odesłania do art. 267 § 1 i 2 k.k.

2. Ocenę projektowanej propozycji należy poprzedzić wskazaniem, że art. 7 dyrektywy 2013/40 nakłada na państwa członkowskie obowiązek podejmowania środków niezbędnych do zagwarantowania, by umyślne wytwarzanie, sprzedaż, dostarczanie w celu użycia, przywóz, rozpowszechnianie lub udostępnianie w inny sposób niektórych narzędzi było karalne jako przestępstwo, jeżeli zostało dokonane bezprawnie i umyślnie w celu popełnienia któregokolwiek z przestępstw, o których mowa w art. 3–6 dyrektywy – co najmniej w przypadkach, które nie są przypadkami mniejszej wagi. Chodzi tu mianowicie o przestępstwa: niezgodnego z prawem dostęp do systemów informatycznych (art. 3), niezgodnej z prawem ingerencji w system (art. 4), niezgodnej z prawem ingerencji w dane (art. 5) oraz niezgodnego z prawem przechwytywania środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego (art. 6 dyrektywy 2013/40). Większość opisanych w tych przepisach zachowań znajduje odzwierciedlenie w rozdziale XXXIII Kodeksu karnego.

Komisja Europejska dostrzegła jedynie, że art. 269b § 1 k.k. nie zawiera odesłania do art. 267 § 1 i 2 k.k., które odzwierciedlają art. 3 i częściowo art. 6 dyrektywy 2013/40. Wskazała wprost, że umyślne wytwarzanie, zbywanie, pozyskiwanie do użytku, import, dystrybucja lub udostępnianie w inny sposób niektórych narzędzi z zamiarem ich wykorzystania do „niezgodnego z prawem dostępu do systemów informatycznych” (art. 3 dyrektywy 2013/40) oraz do „niezgodnego z prawem przechwytywania danych komputerowych” (art. 6 dyrektywy 2013/40) nie są objęte zakresem polskiego prawa karnego. Stwierdzenie Komisji Europejskiej w powyższym zakresie jest trafne. Brak wskazania w treści art. 269b § 1 k.k. odwołania do art. 267 § 1 k.k. skutkuje tym, że poza zakresem kryminalizacji pozostaje czyn polegający na wytwarzaniu, pozyskiwaniu, zbywaniu lub udostępnianiu innym osobom urządzenia lub programu komputerowego przystosowane do „uzyskania dostęp do informacji dla niego nieprzeznaczonej”, a zatem zachowanie ułatwiające realizację znamion przestępstwa określonego w art. 267 § 1 k.k. Zbieżna konkluzja dotyczy pominięcia w treści art. 269b § 1 k.k. odwołania do art. 267 § 2 k.k. Ten ostatni przepis kryminalizuje zachowanie polegające na uzyskaniu dostępu do całości lub części systemu informatycznego bez stosownego uprawnienia. Obecnie, wbrew art. 6 dyrektywy 2013/40, wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzenia lub programu komputerowego służącego do takiego dostępu nie jest objęte przepisami prawa karnego. W celu zmiany takiego stanu prawnego, w szczególności poprawy bezpieczeństwa dostępu do danych przetwarzanych w systemach informatycznych, Ministerstwo Sprawiedliwości trafnie przewidziało uzupełnienie treści art. 269b § 1 k.k. o odwołanie do art. 267 § 2 k.k.

O ile sama idea objęcia zakresem kryminalizacji zachowa wskazanych w art. 7 dyrektywy 2013/40 zasługuje na ocenę pozytywną, o tyle budzi zastrzeżenia propozycja nowelizacji art. 269b § 1 k.k., która w dalszym ciągu przewiduje możliwość realizacji typu czynu zabronionego opisanego w art. 269b § 1 k.k. zarówno z zamiarem bezpośrednim, jak i ewentualnym. Przepis art. 7 dyrektywy 2013/40 stanowi, że państwa członkowskie podejmują środki prawne, by „umyślne wytwarzanie, sprzedaż, dostarczanie w celu użycia, przywóz, rozpowszechnianie lub udostępnianie w inny sposób jednego z następujących narzędzi było karalne jako przestępstwo”. W świetle przywołanego przepisu mowa jest zatem o zamiarze bezpośrednim kierunkowym, i w takim zakresie należy ukształtować propozycję legislacyjną czyniącą zadość przepisowi unijnemu.

Opracował: prof. dr hab. Andrzej Sakowicz

1. J. Giezek, (w:) J. Giezek (red.), Kodeks karny. Część szczególna. Komentarz, Warszawa 2021, Lex, komentarz do art. 269b k.k. [↑](#footnote-ref-1)
2. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz. U. L 218 z 14.8.2013, s. 8–14. [↑](#footnote-ref-2)