Pojęcia kluczowe: *dywersja, przestępstwo, sabotaż, wojna hybrydowa*

Robert Rynkun-Werner

Dywersja i sabotaż, czyli nowe ujęcie przestępstwa szpiegostwa w polskim prawie karnym

Abstrakt

Przedmiotem artykułu jest przybliżenie założeń związanych z nowelizacją art. 130 k.k., która dokonała się w 2023 r., a odnosiła się m.in. do nowego zdefiniowania przestępstwa szpiegostwa. Wobec nasilenia się w ostatnim czasie na terytorium Polski działań takich jak dywersja i sabotaż, szczególnie istotne stało się również przybliżenie podstawowych zagadnień w tej materii, które, co istotne, objęte zostały penalizacją karną.

I. Wprowadzenie

W wyniku licznych zdarzeń naruszających i zagrażających bezpieczeństwu państwa polskiego, co ma bezpośredni związek z trwającym konfliktem zbrojnym na Ukrainie oraz zaangażowaniem Polski w pomoc humanitarną i militarną na jej rzecz, w przestrzeni medialnej coraz częściej pojawiają się takie pojęcia jak dywersja czy sabotaż. Pojęcia te choć znane od wieków, początkowo związane z oporem robotników, z czasem przekształciły się w elementy działań wojennych, które nabrały szczególnego znaczenia w zakresie bezpieczeństwa państwa, które nie jest wprawdzie stroną konfliktu, ale w sposób zdecydowany wspiera jedną z walczących stron i pomaga jej[1]. W ten sposób staje się państwem wrogim dla agresora, co w konsekwencji prowadzi do wojny hybrydowej, w której dywersja i sabotaż są podstawowymi działaniami konfrontacyjnymi. Dostrzegł to polski ustawodawca, który w 2023 r. dokonał zmian w ustawie Kodeks karny oraz w szeregu innych aktów prawa odnoszących się do systemu bezpieczeństwa państwa, podejmując próbę dostosowania przepisów prawa karnego dotyczących szpiegostwa do aktualnej sytuacji geopolitycznej.

1 M. Romański, *O sabotażu i dywersji w świetle polskiego ustawodawstwa po 1944 roku*, „Czasopismo Prawno-Historyczne", Tom LXV Toruń 2013, z. 1, s. 312.

DOI: 10.54383/0031-0344.2026.08.3

II. Zmiany w obliczu realnego zagrożenia

Nowelizacja, w szczególności nowa treść art. 130 k.k., wprowadzona została na mocy ustawy z 17.08.2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw[2]. Projektodawcy, uzasadniając konieczność wprowadzenia zmian, wskazywali na wysokie zagrożenie nowymi konfliktami zbrojnymi oraz agresywnymi działaniami niemilitarnymi, nasileniem działań szpiegowskich i stałymi modyfikacjami sposobu działania potencjalnych sprawców czynów zabronionych opisanych w pierwotnej wersji art. 130 k.k. Celem zmian było dostosowanie przepisów k.k. do aktualnej sytuacji geopolitycznej[3]. Zasadniczym ich kierunkiem było usprawnienie zwalczania przestępstwa szpiegostwa, które zdaniem projektodawców do czasu nowelizacji z 2023 r. miało napotykać szereg problemów dowodowych i skutkować uniewinnieniami sprawców czynów objętych tą normą prawną. Powołując się na powyższe argumenty, projektodawcy, jak podnosił w swojej krytycznej opinii do projektu zmian Sąd Najwyższy, nie wskazali jednak żadnych badań dotyczących orzecznictwa sądów powszechnych, które mogłyby je potwierdzać. Ponadto SN ocenił argumentację projektodawców jako nazbyt ogólnikową[4]. Równie istotnym celem zmian był ich walor prewencyjny, a więc drastyczne zwiększenie sankcji karnych w tej materii[5]. W odniesieniu do propozycji zwiększenia kar z kolei SN uznał je za wręcz populistyczne[6]. SN zwracał uwagę na naruszenie zasady proporcjonalności owych propozycji, które nie znajdowały żadnego racjonalnego wytłumaczenia. Zmiany k.k. w swojej zasadniczej części odnosiły się do wprowadzenia nieumyślnej postaci szpiegostwa i penalizacji przygotowania, co miało usprawnić zwalczanie tego rodzaju przestępstw oraz skutkować pozytywnym wpływem na bezpieczeństwo i interesy RP. Z całą pewnością nowelizacja miała na celu wywołanie efektu prewencji szczególnej, gdyż jak do tej pory, co pokazywały statystyki, przestępstwo szpiegostwa należało do kategorii przestępstw marginalnych i nie wszyscy przedstawiciele świata polityki oraz wymiaru sprawiedliwości do końca rozumieli, po pierwsze, na czym ono polega, a po wtóre, nie doceniali dalekosiężnych negatywnych skutków, które wywołuje[7].

2 Dz.U. poz. 1834.

3 Uzasadnienie do projektu Druk 3232 oraz Druk 3232 A, s. 13, https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=3232 (dostęp: 25.11.2025 r.).

4 Opinia SN do projektu zmiany ustawy k.k. i innych ustaw, https://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=3232.

5 Tamże, s. 3.

6 Tamże; zob. też S. Hoc, *Szpiegostwo w znowelizowanym Kodeksie karnym*, „Nowa Kodyfikacja Prawa Karnego" Tom LXVII, Wrocław 2025, s. 130.

7 G. Ocieczek, *Wybrane zagadnienia związane z przestępstwem szpiegostwa*, „Consilium Iuridicum" 2024/3(11), s. 83.

 DOI: 10.54383/0031-0344.2026.08.3

III. Szpiegostwo po nowemu

Z uwagi na szczególne znaczenie omawianej regulacji oraz stosunkowo niewielkie wykorzystanie jej w dotychczasowej praktyce sądowej, zasadne jest przytoczenie treści nowych regulacji w pełnym zakresie. Zgodnie z aktualnym brzmieniem art. 130 § 1 k.k. „kto bierze udział w działalności obcego wywiadu albo działa na jego rzecz, przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 5. Zgodnie zaś z treścią § 2 art. 130 k.k. kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, udziela temu wywiadowi wiadomości, której przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 8 albo karze dożywotniego pozbawienia wolności. § 3. Kto zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej albo w celu udzielenia obcemu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, gromadzi je lub przechowuje lub wchodzi do systemu informatycznego w celu ich uzyskania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 4. Kto działalność obcego wywiadu, o której mowa w § 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności na czas nie krótszy od lat 10 albo karze dożywotniego pozbawienia wolności. § 5. Funkcjonariusz publiczny oraz osoba pełniąca dyspozycyjnie terytorialną służbę wojskową, dopuszczający się czynu, o którym mowa w § 1, podlega karze pozbawienia wolności na czas nie krótszy od lat 8 albo karze dożywotniego pozbawienia wolności. § 6. Kto bierze udział w działalności obcego wywiadu nieskierowanej przeciwko Rzeczypospolitej Polskiej prowadzonej na jej terytorium bez zgody właściwego organu udzielonej na podstawie odrębnych przepisów, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. **§ 7. Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, dokonuje dywersji, sabotażu lub dopuszcza się przestępstwa o charakterze terrorystycznym, podlega karze pozbawienia wolności na czas nie krótszy od lat 10 albo karze dożywotniego pozbawienia wolności**. **§ 8. Kto czyni przygotowania do przestępstwa określonego w § 7, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.** § 9. Kto, biorąc udział w działalności obcego wywiadu albo działając na jego rzecz, prowadzi dezinformację, polegającą na rozpowszechnianiu nieprawdziwych lub wprowadzających w błąd informacji, mając na celu wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska, albo skłonienie organu władzy publicznej Rzeczypospolitej Polskiej, państwa sojuszniczego lub organizacji międzynarodowej, której członkiem jest Rzeczpospolita Polska, do podjęcia lub zaniechania określonych czynności, podlega karze pozbawienia wolności na czas nie krótszy od lat 8".

DOI: 10.54383/0031-0344.2026.08.3

Jak z powyższego wynika, w stosunku do poprzedniego stanu prawnego dodano sześć nowych podstawowych typów czynów zabronionych i wprowadzono karalność przygotowania jednego z nich. Czyny zabronione stypizowane w § 1, 2, 4, 5, 7, 9 stanowią zbrodnie, a w § 3, 6 oraz przygotowanie z § 8 występki[8]. Przedmiotem przestępstwa z art. 130 k.k. jest bezpieczeństwo wewnętrzne i zewnętrzne oraz obronność i gospodarka państwa. Jest to przestępstwo powszechne, można je popełnić umyślnie w obu postaciach zamiaru. Istotą przestępstw z art. 130 k.k. jest czynność brania udziału w działalności obcego wywiadu lub działania na jego rzecz, czyli dokonywanie różnych zachowań przez sprawcę, nawet formalnie niepozostającego w strukturach tego wywiadu, ale skierowanych przeciwko RP[9].

IV. Dywersja, sabotaż, akt terrorystyczny

Przedmiotem szczególnego zainteresowania niniejszego opracowania jest treść art. 130 § 7 k.k., który penalizuje branie udziału w działalności obcego wywiadu oraz działanie na jego rzecz, poprzez dokonywanie dywersji, sabotażu oraz przestępstwa o charakterze terrorystycznym. Wprowadzono zatem w § 7 art. 130 k.k. nowy typ podstawowy przestępstwa szpiegostwa. W dotychczas obowiązującym stanie prawnym nie było regulacji odnoszącej się bezpośrednio do dywersji i sabotażu. Pewnym wyjątkiem był „sabotaż komputerowy", o którym mowa w art. 269 § 1 k.k., polegający na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu danych informatycznych[10]. Przy czym chodzi tu o dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. Przykładowo odnosić się to może do: danych PESEL; systemu sterowania ruchem lotniczym, kolejowym czy energetyką. Jest to jednak określenie doktrynalne, a nie legalna definicja sabotażu komputerowego jako przestępstwa. Szczególnego znaczenia w przypadku dywersji, sabotażu czy aktu terrorystycznego nabiera działanie ukierunkowane na niszczenie infrastruktury krytycznej, czyli tych obszarów, które są identyfikowane jako kluczowe dla funkcjonowania państwa. Legalną definicję infrastruktury krytycznej zawiera art. 3 pkt 2 ustawy z dnia 26.04.2007 r. o zarządzaniu kryzysowym[11]. Zgodnie z jego treścią infrastrukturą krytyczną są 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

8 M. Filipczak (w:) *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, art. 130.

9 M. Budyn-Kulik (w:) *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2025, art. 130.

10 A. Behan (w:) *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, art. 269; zob. też M. Romański, *O sabotażu*…, s. 311.

11 T.j. Dz.U. z 2023 r. poz. 122.

 DOI: 10.54383/0031-0344.2026.08.3

instytucji i przedsiębiorców. Ustawa wymienia enumeratywnie owe systemy, do których przykładowo należą systemy: zaopatrzenia w energię, surowce energetyczne i paliwa; łączności; sieci teleinformatycznych; finansowe; zaopatrzenia w żywność i wodę; transportowe czy ochrony zdrowia[12]. Można zgodzić się z występującym w doktrynie poglądem, że oba te znamiona (branie udziału i działanie na rzecz) czynnościowe zostały przez ustawodawcę ujęte dość niezręcznie. W obu przypadkach lepszym rozwiązaniem byłoby użycie słowa „popełnia"[13]. Przestępstwo to może być popełnione zarówno przez **działanie**, jak i przez **zaniechanie**. Przestępstwo z § 7 art. 130 k.k. ma charakter indywidualny co do czynu. Jego strona podmiotowa polega na umyślności. Czyn stypizowany w tym przepisie polega na dokonaniu dywersji lub sabotażu lub dopuszczeniu się przestępstwa o charakterze terrorystycznym. W przypadku dokonania dywersji lub sabotażu w grę wchodzą **obie postaci zamiaru**, natomiast w przypadku przestępstwa o charakterze terrorystycznym – tylko **zamiar bezpośredni kierunkowy**[14]. Omawiany czyn zabroniony ma charakter formalny. Do jego znamion nie należy skutek w postaci spowodowania dezorganizacji działań czy zakłócenia funkcjonowania państwa lub faktycznego przeszkodzenia w realizacji planu. Sankcja za udział w takim przestępstwie jest surowa, bowiem sprawca podlega karze na czas nie krótszy od lat 10 albo dożywotniemu pozbawieniu wolności. Dodatkowo, w § 8 art. 130 k.k. ustawodawca wprowadził karalne przygotowanie do tego przestępstwa, którego sankcja została określona w wymiarze od 6 miesięcy do lat 8 pozbawienia wolności.

Ustawodawca, nowelizując k.k., nie wprowadził jednak definicji legalnych przestępstwa dywersji i sabotażu, co prowadzi do konieczności sięgnięcia przede wszystkim do wykładni językowej tych pojęć, zawartej w słowniku języka polskiego. W aktualnej sytuacji geopolitycznej obie formy przestępstwa mają wspólny mianownik, którym jest wojna hybrydowa. Przy czym przez wojnę hybrydową należy rozumieć konflikt, w którym przeciwnik stosuje kombinację środków konwencjonalnych, nieregularnych, terrorystycznych i przestępczych w celu osiągnięcia swoich celów politycznych[15]. Najważniejszym elementem wojny hybrydowej jest jednak wpływanie na społeczeństwo przeciwnika w taki sposób, aby wywarło presję na rząd i wymusiło określone działania lub ustępstwa[16].

Dywersja oznacza działania prowadzone na zapleczu i tyłach wojsk nieprzyjaciela w celu utrudnienia mu prowadzenia akcji na froncie i obniżenia wartości bojowej

12 F. Wyszyński, *Zdatność regulacji prawnokarnych do kompleksowej ochrony paliwowej infrastruktury krytycznej przed cyberprzestępczością*, „ACTA IURIDICA RESOVIENSIA", Rzeszów 2024/2(45), s. 173.

13 M. Budyn-Kulik (w:) *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2025, art. 130.

14 M. Filipczak (w:) *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, art. 130.

15 W. Skomra, K. Wojtasik, *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK* (w:) *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, red. K Wojtasik, D. Szlachter, Warszawa 2025, s. 15.

16 F.G. Hoffman, *Conflict in the 21'st Century: The Rise of Hybrid Wars*, Virginia 2007, https:// www.comw.org/qdr/fulltext/0712hoffman.pdf, s. 14.

jego wojska. Jest to działalność zmierzająca do zakłócenia życia politycznego, administracyjnego i gospodarczego danego państwa oraz osłabienia jego potencjału militarnego dla osiągnięcia określonych celów politycznych[17]. Można zauważyć, że działania dywersyjne mają charakter zaczepny, skryty, zaskakujący, gwałtowny w działaniu i prowadzony na terytorium przeciwnika[18]. Do podstawowych cech działań dywersyjnych zaliczyć można: elastyczność, mobilność, samodzielność, prostotę oraz zmienność stosowanej taktyki. Elastyczność charakteryzuje się dostosowaniem ogółu działań do zaistniałych warunków. Mobilność wyraża się szybkością działania i sprawnością wycofania się z miejsca akcji. Samodzielność przejawia się umiejętnością dokonywania zmian we wcześniej ustalonym planie działania. Natomiast zmienność stosowanej taktyki polega na dostosowaniu działań do zmieniających się okoliczności[19]. Dywersja cechuje się także celowymi działaniami przeprowadzanymi przez zaskoczenie i unikanie bezpośredniej konfrontacji. Przykładami dywersji może być wykolejanie pociągów na istotnych szlakach komunikacyjnych, rozcinanie linii telekomunikacyjnych i światłowodowych, zatruwanie ujęć wodnych i zbiorników wodnych, próby zabójstw ważnych osób w państwie, wysadzanie mostów, podpalenia. Dywersja to także elementy walki ideologicznej, jako element wojny hybrydowej[20]. Dywersję można określić jako dezinformację, manipulację informacjami czy stworzenie fałszywych zagrożeń. To cyberataki na systemy informacyjne państwa.

Sabotaż z kolei to ukryte, zamaskowane działanie mające na celu przeszkodzenie w realizacji jakiegoś planu lub zamierzona dezorganizacja pracy polegająca na niszczeniu maszyn, na uchylaniu się od pracy, wadliwym jej wykonywaniu[21]. Sabotaż jest konkretnym, taktycznym, punktowym oraz szybkim działaniem mającym doprowadzić do fizycznego zniszczenia obiektu lub wywołania zakłócenia w jego funkcjonowaniu. Przykładem sabotażu może być uszkodzenie torów na linii Warszawa––Dorohusk w listopadzie 2025 r. Dywersję i sabotaż łączy skrytość działania. Jednak dla dywersji potrzebne jest wyszkolenie dywersanta, w przypadku zaś sabotażu nie jest to konieczne, bowiem sabotażystą może być każdy. Intencje działania sprawcy mogą być różne, przykładowo względy ideologiczne czy finansowe**.**

W końcu treść § 7 art. 130 k.k. wymienia także **przestępstwo o charakterze terrorystycznym**, którego definicję zawiera słowniczek wyrażeń ustawowych w art. 115

17 *Uniwersalny Słownik języka polskiego*, red. J. Dubisz, Warszawa 2003, t. 1, s. 754.

18 P. Lubiewski, A. Dróżdż, *Dywersja i sabotaż – istota oraz wzajemne relacje*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2021/28, s. 48.

19 R. Jakubczak, B. Wiśniewski, *Ogólna charakterystyka dywersji* (w:) *Właściwości dywersji i jej zwalczania. Zarys problemu*, red. R. Jakubczak, B. Wiśniewski, Warszawa 2006, s. 11.

20 M. Borysiak, *Czym jest akt dywersji? Definicja, przykłady i surowe kary. Prawo przewiduje nawet dożywocie*, „Dziennik Gazeta Prawna", https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/10586625,czym-jest-dywersja-definicja-przyklady-kary-prawo-polska.html (dostęp: 25.11.2025 r.).

21 *Uniwersalny Słownik języka polskiego*, red. S. Dubisz, PWN, Warszawa 2003, t. 3, s. 1124.

 DOI: 10.54383/0031-0344.2026.08.3

§ 20 k.k. Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: poważnego zastraszenia ludzi; zmuszenia organu władzy publicznej RP lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej – a także groźba popełnienia takiego czynu. Jak to już podkreślono, ustawodawca w § 8 art. 130 k.k. zdecydował się na karalność także przygotowania, co z punktu widzenia ochrony najistotniejszych interesów państwa wydaje się całkowicie uzasadnione. Sprawca może jednak uniknąć kary za usiłowanie dokonania przestępstwa z art. 130 § 7 k.k., o ile dobrowolnie poniechał dalszej działalności i ujawnił wobec organu powołanego do ścigania przestępstw wszystkie istotne okoliczności popełnionego czynu. W tym przypadku w odpowiedni sposób będzie miał zastosowanie przepis art. 17 § 2 k.k. o niepodleganiu karze za dobrowolne odstąpienie od przygotowania. Zgodnie zaś z treścią § 2 art. 131 k.k. nie podlega karze za przestępstwo określone w art. 128 § 2, art. 129 lub art. 130 § 3, 6 i 8, kto dobrowolnie poniechał dalszej działalności i podjął istotne starania zmierzające do zapobieżenia popełnieniu zamierzonego czynu zabronionego oraz ujawnił wobec organu powołanego do ścigania przestępstw wszystkie istotne okoliczności popełnionego czynu. Możliwy jest zbieg kumulatywny z przepisami typizującymi przestępstwa przeciwko ochronie informacji, a także zasadniczo z każdym innym, którego realizacja następuje w ramach czynu z art. 130 k.k., z wyjątkiem art. 288 k.k., który jest konsumowany przez zastosowanie art. 130 k.k.

V. Sprawcy i ich metody

Przedłużający się konflikt zbrojny na Ukrainie przeniósł się poprzez wojnę hybrydową prowadzoną przez Rosję na terytorium Europy, w tym – co oczywiste – i Polski. W ostatnich latach dochodzi do licznych działań o charakterze dywersyjnym czy też sabotażowym, o których wiedza jest powszechna i ogólnodostępna na skutek przekazów medialnych czy komunikatów rządowych zaatakowanych państw. Do najbardziej spektakularnych i niebezpiecznych działań można zaliczyć: kryzys na granicy polsko-białoruskiej trwający od jesieni 2021 r.; pożar w hali Marywilska w Warszawie w maju 2024 r.; zatrzymanie 9 osób, których zadaniem było zbieranie informacji na temat transportów z uzbrojeniem jadących przez Polskę; rozmieszczenie kamer rejestrujących ruch na drogach i transmitujących obraz do sieci – znaleziono około 50 tego typu urządzeń; prowadzenie aktywności propagandowej w cyberprzestrzeni, której celem jest rozbudzanie emocji wokół relacji polsko-ukraińskiej, budowanie nieprzychylnego stanowiska wobec Ukrainy, wywoływanie niechęci wobec rządu; dewastacja pojazdów osób oficjalnych lub dziennikarzy oraz duża, ponadnormatywna liczba pożarów; zatrzymanie osób,

DOI: 10.54383/0031-0344.2026.08.3

które przygotowywały się do ataków z wykorzystaniem materiałów wybuchowych na bazy wojskowe oraz transporty z uzbrojeniem; pożary zakładu produkującego amunicję artyleryjską czy pociski do systemów obrony przeciwlotniczej; zakłócenia przed Igrzyskami Olimpijskimi w Paryżu w 2024 r. i na początku ich trwania; zatkania rur wydechowych w samochodach w Niemczech na masową skalę; testowanie możliwości wywołania eksplozji i pożarów w firmach kurierskich, na lotniskach i w samolotach. W połowie lipca 2024 r. w Warszawie nadano cztery paczki, z których dwie miały drogą lotniczą dotrzeć do miejsc docelowych. Trzy paczki uległy samozapłonowi[22]; doszło do wysadzenia torów kolejowych w listopadzie 2025 r. w Polsce. I jakkolwiek większość z takich działań nie znalazło jeszcze swojego finału w sądach w postaci prawomocnego wyroku, to ich skala i zasięg powoduje realne zagrożenie dla bezpieczeństwa państwa i jego obywateli. Powyższe w jednoznaczny sposób świadczy o trwającej już od lat wojnie hybrydowej Rosji przeciwko Polsce i innym krajom UE. Zasadniczy problem, jaki występuje przy przestępstwach z art. 130 k.k., dotyczy wykrycia potencjalnych sprawców takich czynów. O ile szpieg zawodowy często wykorzystuje przykrycie dyplomatyczne, co w przypadku wykrycia takiej działalności zasadniczo prowadzi do zastosowania przez państwo środków dyplomatycznych, a więc wydalenia z Polski, o tyle w wojnie hybrydowej większego znaczenia nabierają działania inicjowane i koordynowane przez rosyjskie służby specjalne wymierzone przeciwko RP i państwom NATO, poprzez werbowanie przede wszystkim młodych ludzi pochodzących z państw byłego ZSRR, m.in. Ukrainy czy Białorusi, pod fałszywą flagą. Nader często potencjalni sprawcy mają powiązania ze środowiskami przestępczymi i kierują się przede wszystkim kwestiami finansowymi. Ich działalność nie wymaga jednak więzi organizacyjnej łączącej ich z obcym wywiadem[23]. Osoby te nie zawsze kierują się pobudkami ideologicznymi, często deklarują poglądy antyrosyjskie, co i tak nie przeszkadza im w realizacji działań *de facto* przeciwko Polsce. Dywersanci działający dla rosyjskich służb wywiadowczych komunikują się najczęściej przez media społecznościowe i komunikatory, takie jak Telegram, a wynagrodzenie odbierają głównie w kryptowalutach, co znacznie utrudnia wykrycie prawdziwych mocodawców[24]. Sprawcy często wykorzystują sieci pośredników, botnety (zainfekowane komputery szkodliwym oprogramowaniem) lub fałszywe ślady, co praktycznie uniemożliwia wskazanie atakującego. W przypadku aktów fizycznego sabotażu, takich jak uszkodzenie kabli podmorskich czy rurociągów, sprawcy mogą upozorować niewyjaśnioną awarię czy działania grup terrorystycznych. To sprawia, że zaatakowane państwo ma ograniczone możliwości reakcji. Sabotażysta prowadzi działania destabilizujące i unika oficjalnej konfrontacji

22 Wyrok Sądu Okręgowego we Wrocławiu z 21.02.2025 r. (III K 339/24), LEX nr 3843269.

23 J. Kulesza (w:) *Kodeks karny. Część szczególna. Komentarz*, red. M. Królikowski, R. Zawłocki, Warszawa 2023, t. 1, art. 117–221, s. 109.

24 K. Głodowska, *Rosyjska dywersja coraz większym problemem w Polsce. Komunikat ABW*, https://wydarzenia.interia.pl/kraj/news-rosyjska-dywersja-coraz-wiekszym-problemem-w-polsce-komunika,nId,7843612 (dostęp: 30.11.2025 r.).

 DOI: 10.54383/0031-0344.2026.08.3

zbrojnej[25]. Z kolei cyberprzestrzeń umożliwia przeprowadzenie ataku z dowolnego miejsca na świecie, co utrudnia identyfikację sprawców, a w konsekwencji ich ukaranie. Ataki na infrastrukturę krytyczną są skuteczne nie tylko dlatego, że powodują ogromne straty, lecz także dlatego, że sprawcy mogą działać anonimowo i bezkarnie.

VI. Trudności dowodowe

Działania szpiegowskie, takie jak dywersja, sabotaż czy terroryzm, dokonywane są w warunkach poufności, często organizowane bez osobistej styczności zleceniodawcy ze zleceniobiorcą. Jak to już podkreślono, kontakt odbywa się przede wszystkim przy pomocy sieci teleinformatycznych. Powoduje to trudności w wykryciu takich działań, w szczególności w fazie ich przygotowania. Stąd też postępowanie przygotowawcze w tego typu sprawach to przede wszystkim etap czynności operacyjno-rozpoznawczych, w tym wywiadowczych, prowadzonych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, prokuraturę i policję. Prowadzenie czynności operacyjnych musi być zakończone zebraniem i zabezpieczeniem dowodów w rozumieniu przepisów k.p.k., tak aby można było je wykorzystać w procesie karnym. Stąd też prowadzenie takiego postępowania obarczone jest wyższą skalą trudności, tak dla prowadzącego je prokuratora, ale także w konsekwencji dla broniącego podejrzanego obrońcy, którego wpływ na owe czynności na tym etapie postępowania jest znikomy, o ile nie żaden. Tym bardziej, jak to już podkreślono, *gros* dowodów jest niejawnych i opiera się wyłącznie na czynnościach operacyjnych, w tym na zeznaniach, np. świadka anonimowego, w oparciu o art. 184 k.p.k. Problemem w tego typu postępowaniach jest zatem realne zachowanie standardów rzetelnego postępowania sądowego, w szczególności w zakresie prawa do obrony. Problemem jest tu wspomniana kwestia niejawnych dowodów i powoływania się na klauzule tajne i ściśle tajne, m.in. zgodnie z art. 5 ust. 1 i 2 ustawy o ochronie informacji niejawnych[26]. Nie bez znaczenia pozostaje w tym kontekście treść art. 8 ust. 1 przedmiotowej ustawy, gdzie informacje niejawne, którym nadano określoną klauzulę tajności:

- mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;
- muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;

25 W. Skomra, K. Wojtasik, *Infrastruktura*…, s. 17.

26 Ustawa z dnia 5.08.2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2025 r. poz. 1209).

- muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Zgodnie zaś z treścią art. 27 ust. 6 ustawy z dnia 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego Kontrola operacyjna prowadzona jest niejawnie i polega na:

- uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
- uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
- uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
- uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
- uzyskiwaniu dostępu i kontroli zawartości przesyłek[27]. ABW zgodnie z art. 28 ABW.U. może także uzyskiwać niezbędne do realizacji zadań dane niestanowiące treści odpowiednio komunikatu elektronicznego przesyłanego w ramach świadczonej publicznie dostępnej usługi telekomunikacyjnej, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:
  - art. 45 ust. 1 i art. 49 ustawy z dnia 12.07.2024 r. – Prawo komunikacji elektronicznej, zwane dalej „danymi telekomunikacyjnymi",
  - art. 82 ust. 1 pkt 1 ustawy z dnia 23.11.2012 r. – Prawo pocztowe (Dz.U. z 2025 r. poz. 366), zwane dalej „danymi pocztowymi",
  - art. 18 ust. 1–5 ustawy z dnia 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2024 r. poz. 1513), zwane dalej „danymi internetowymi" – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą. Kontrole nad pozyskiwaniem danych sprawuje Sąd Okręgowy w Warszawie.

Jeszcze przed wszczęciem postępowania karnego w ramach czynności operacyjno-rozpoznawczych zmierzających do udokumentowania tych przestępstw albo ustalenia tożsamości osób uczestniczących w tych przestępstwach lub przejęcia przedmiotów przestępstwa Szef ABW może zarządzić niejawne nadzorowanie wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, jeżeli nie stworzy to zagrożenia dla życia lub zdrowia ludzkiego (art. 30 ust. 1 ABW.U.). Przy wykonywaniu powyższych czynności mogą być prowadzone niejawne czynności

27 Ustawa z dnia 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2025 r. poz. 902 ze. zm.).

 DOI: 10.54383/0031-0344.2026.08.3

operacyjne, o których mowa w art. 27 ust. 6 ABW.U., o czym już wspomniano. Z punktu widzenia tematyki opracowania istotne wydaje się uprawnienie ABW oceny bezpieczeństwa systemów teleinformatycznych. Zgodnie z treścią przepisu art. 32a ust. 1 ABW.U. w celu zapobiegania, przeciwdziałania i zwalczania zdarzeń o charakterze terrorystycznym lub uprawdopodabniających popełnienie przestępstwa szpiegostwa, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26.04.2007 r. o zarządzaniu kryzysowym, lub danych przetwarzanych w tych systemach oraz rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców, ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych, zwaną dalej „oceną bezpieczeństwa". Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu teleinformatycznego w celu identyfikacji podatności, przez które rozumie się słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie, wpływających na integralność, poufność, rozliczalność i dostępność tego systemu. Podobne uprawnienie ma ABW w zakresie wczesnego ostrzegania o zagrożeniach występujących w sieci Internet (art. 32aa ABW.U.). Czynności operacyjne w interesującym nas zakresie prowadzi także Służba Kontrwywiadu Wojskowego[28]. Jak z powyższego wynika, nowe formy przestępstwa szpiegostwa, jak też specyfika środowiska, w którym podejmowane są działania dywersyjne czy sabotażowe, wymagają szczególnych metod i środków zmierzających do ich wykrycia.

VII. Zakończenie

Wprowadzone w 2023 r. zmiany w art. 130 k.k. co do zasady należy ocenić pozytywnie. Pewne wątpliwości natury systemowej budzą jednak zmiany odnoszące się do radykalnego podniesienia wysokości sankcji karnych, których efektem był bardziej populizm, a nie ich realizm. I jakkolwiek po trzech latach od nowelizacji art. 130 k.k. bardziej zrozumiały może wydawać się cel prewencyjny takich uregulowań, to nadal nowe wymiary kar, jak i wynikające z tego ograniczenie swobody sędziowskiej, zdają się stać w sprzeczności ze współczesnymi zasadami procesu karnego i celami polityki karnej państwa demokratycznego. Nie ma wątpliwości, że dla większości obywateli

28 Ustawa z dnia 9.06.2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz.U. z 2024 r. poz. 1405 ze zm.), zob. w szczególności art. 31–39 ustawy.

polskich działalność wywiadu rosyjskiego od lat skierowana jest przeciwko jej interesom, co było i jest faktem notoryjnym powszechnie znanym, niewymagającym dowodzenia[29]. Cechą charakterystyczną tych działań jest skrytość i hermetyczność organizatorów i sprawców. Nie oznacza to oczywiście, że organy ścigania są skazane na porażkę w trwającej wojnie hybrydowej. Z pozyskanych z Prokuratury Krajowej informacji wynika, że liczba postępowań zarejestrowanych o czyn z art. 130 k.k. za okres od 1.10.2023 r. do 7.12.2025 r. wynosiła 117, ale już liczba postępowań wszczętych o ten czyn w powyższym okresie wyniosła 66[30]. Niestety trwający konflikt zbrojny na Ukrainie i jednoznaczna postawa Polski powoduje coraz większe zagrożenie działaniami szpiegowskimi. Celowe jest zatem podniesienie skuteczności działania wywiadu, kontrwywiadu, prokuratury, policji czy ABW w zakresie zwalczania działalności szpiegowskiej, co można osiągnąć przez odpowiedni poziom pracy operacyjnej, wykorzystanie środków technicznych i osobowych, współdziałanie pionu operacyjnego i śledczego[31]. Pomimo istniejących realnych zagrożeń, powyższe działania, a więc zasadniczo pozyskiwanie dowodów, muszą być jednak realizowane przy zachowaniu wszelkich standardów demokratycznego państwa prawnego. Dotyczy to tak zdobywania, jak i wykorzystywania dowodów w procesie karnym.

adw. dr Robert Rynkun-Werner
Adwokat, Warszawa, doktor nauk prawnych.
Advocate, Warsaw, Doctor of Laws.
ORCID:0000-000106559-7731

29 Pogląd taki zawarł już w 2017 r. Sąd Apelacyjny w Warszawie w wyroku z 24.11.2017 r. (II AKa 269/17), LEX nr 2446547.

30 Pismo z Biura Prezydialnego Prokuratury Krajowej z dnia 10.12.2025 r. w odpowiedzi na zapytanie autora – źródła własne.

31 S. Hoc, *Szpiegostwo*…, s. 120.

 DOI: 10.54383/0031-0344.2026.08.3

Abstract

Keywords: *subversion, crime, sabotage, hybrid warfare*

Subversion and sabotage, or new challenges of the criminal procedure

This article examines the assumptions behind the 2023 amendment to Article 130 of the Penal Code, which, among other things, attempted to redefine the crime of espionage. Given the recent increase in activities such as sabotage and diversion in Poland, it has become particularly important to address the fundamental issues in the matter of these crimes, which – importantly - have been subjected to criminal penalties.

Bibliografia

1. **Behan Adam** (w:) *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, art. 269
2. **Borysiak Marta,** *Czym jest akt dywersji? Definicja, przykłady i surowe kary. Prawo przewiduje nawet dożywocie*, „Dziennik Gazeta Prawna", https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/10586625,czym-jest-dywersja-definicja-przyklady-kary-prawo-polska.html (dostęp: 25.11.2025 r.).
3. **Budyn-Kulik Magdalena** (w:) *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2025, art. 130
4. **Filipczak Mateusz** (w:) *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, art. 130
5. **Głodowska Karolina,** *Rosyjska dywersja coraz większym problemem w Polsce. Komunikat ABW*, https://wydarzenia.interia.pl/kraj/news-rosyjska-dywersja-coraz-wiekszym-problemem-w-polsce-komunika,nId,7843612 (dostęp: 30.11.2025 r.)
6. **Hoc Stanisław,** *Szpiegostwo w znowelizowanym Kodeksie karnym*, „Nowa Kodyfikacja Prawa Karnego" Tom LXVII, Wrocław 2025
7. **Hoffman Frank,** *Conflict in the 21'st Century: The Rise of Hybrid Wars*, Virginia 2007, https:// www.comw.org/qdr/fulltext/0712hoffman.pdf
8. **Jakubczak Ryszard, Wiśniewski Bernard,** *Ogólna charakterystyka dywersji* (w:) *Właściwości dywersji i jej zwalczania. Zarys problemu*, red. R. Jakubczak, B. Wiśniewski, Warszawa 2006
9. **Kulesza Jan** (w:) *Kodeks karny. Część szczególna. Komentarz*, red. J. Kulesza, Warszawa 2025, t. 1

10. **Lubiewski Paweł, Dróżdż Aneta,** *Dywersja i sabotaż – istota oraz wzajemne relacje*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2021/28
11. **Ocieczek Grzegorz,** *Wybrane zagadnienia związane z przestępstwem szpiegostwa*, „Consilium Iuridicum" 2024/3(11)
12. **Romański Mirosław,** *O sabotażu i dywersji w świetle polskiego ustawodawstwa po 1944 roku*, „Czasopismo Prawno-Historyczne", Tom LXV, 2013/1
13. **Skomra Witold, Wojtasik Karolina,** *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK* (w:) *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, red. K Wojtasik, D. Szlachter, Wydawnictwo ABW, Warszawa 2025
14. **Wyszyński Filip,** *Zdatność regulacji prawnokarnych do kompleksowej ochrony paliwowej infrastruktury krytycznej przed cyberprzestępczością*, ACTA IURIDICA RESOVIENSIA, Rzeszów 2024/2(45)

 DOI: 10.54383/0031-0344.2026.08.3