sił i środków, umożliwiającego zlikwidowanie tej przewagi, którą posiadają cyberprzestępcy.

Z każdym dniem, z każdą chwilą w sieci znajduje się coraz więcej użytkowników. Co za tym idzie, zwiększa się liczba przestępstw i liczba ofiar. Z całą pewnością uregulowanie kwestii prawa cybernetycznego stanowi największe wyzwanie dla prawa karnego w XXI wieku.

CZASOPISMO PRAWA KARNEGO I NAUK PENALNYCH
Rok IV: 2000, z. 1 ISSN 1506–1817

PIOTR KARDAS

PRAWNOKARNA OCHRONA INFORMACJI W POLSKIM PRAWIE KARNYM Z PERSPEKTYWY PRZESTĘPSTW KOMPUTEROWYCH

ANALIZA DOGMATYCZNA I STRUKTURALNA W ŚWIETLE AKTUALNIE OBOWIĄZUJĄCEGO STANU PRAWNEGO

I. UWAGI WPROWADZAJĄCE

1. Rozwój nowoczesnych technologii w dziedzinie gromadzenia i przetwarzania danych, wykorzystywanych coraz powszechniej we wszystkich prawie sferach życia, sprawia, iż w coraz większym stopniu funkcjonowanie jednostki w społeczeństwie „rewolucji informacyjnej"[1] uzależnione jest od

[1] W literaturze prawniczej, politologicznej, ekonomicznej i socjologicznej współczesne społeczeństwo określa się często mianem „globalnego społeczeństwa informatycznego" — zob. m.in. A. Toffler, H. Toffler, *Budowa nowej cywilizacji. Polityka trzeciej fali*, Poznań 1996, s. 29 i n.; A. Pawłowska, *Władza i uczestnictwo polityczne w społeczeństwie informacyjnym*, Lublin 1995, s. 12 i n.; A.M. Wilk, *Państwo w dobie społeczeństwa informacyjnego — perspektywa strategicznych przemian* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 185 i n.; A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 16 i n.; W. Cwalina, *Marketing polityczny w Internecie* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 309 i n.; R. Skubisz, *Internet — ku społeczeństwu przyszłości* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 11 i n.; S. Stanisławska–Kloc, *Przedmiot prawa autorskiego* (w:) *Prawo autorskie a postęp techniczny*, red. J. Barta, R. Markiewicz, Kraków 1999, s. 15 i n.; J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 15 i n.; U. Sieber, *Przestępczość komputerowa i prawnokarna ochrona prawa do informacji w międzynarodowej społeczności informacji i ryzyka* (w:) *Prawo karne i proces karny wobec nowych form i technik przestępczości*, red. H.–J. Hirsch, P. Hofmański, E.W. Pływaczewski, C. Roxin, Białystok 1997, s. 223 i n.

dostępu do informacji gromadzonej w specjalnych systemach. We współczesnym świecie informacja staje się dobrem nader istotnym, zaś możliwość jej uzyskania oraz wykorzystywania jest z jednej strony warunkiem funkcjonowania jednostki w zbiorowości, z drugiej strony zaś stwarza możliwość osiągania wymiernych korzyści, porównywalnych do tych, jakie w społeczeństwie tradycyjnym uzyskiwano z praw majątkowych.[2] W ostatnich kilkunastu latach dokonała się zasadnicza zmiana statusu informacji, połączona z niezwykle dynamicznym wzrostem jej gospodarczego znaczenia.[3] Informacja coraz częściej traktowana jest jako produkt, specyficzny towar, do którego znajdują zastosowanie wypracowane przez stulecia zasady wymiany. Zarazem jednak nie straciła ona swojej klasycznej funkcji. Życie zawodowe i prywatne człowieka staje się coraz bardziej uzależnione od dostępu do informacji, gromadzonej, przetwarzanej i przesyłanej przy pomocy nowoczesnych technologii cyfrowych. To uzależnienie jednostki od nowoczesnych źródeł informacji stanowi konsekwencję postępu technicznego, jego przyczyny zdają się jednak tkwić głęboko w samej strukturze społecznej.[4] Jak podkreśla M. Safjan, „jednostka uwikłana jest we współczesnym świecie w aktywności, które *per se* stwarzają konieczność gromadzenia (informacji) danych osobowych. Bez tworzenia baz informatycznych funkcjonowanie jednostki staje pod znakiem zapytania — dotyczy to wszystkich sfer aktywności: od urodzenia po śmierć, od przedszkola do zakładu pracy. Bez danych dotyczących stanu cywilnego, miejsca zamieszkania, wykształcenia, konta bankowego, polisy ubezpieczeniowej, numeru ewidencji podatkowej i ewidencji ludności — jednostka nie istnieje jako podmiot relacji społecznych poddanych prawnej reglamentacji".[5] Rozwój nowoczesnych technologii gromadzenia i przetwarzania danych spra-

[2] Por. W. Wróbel, *Uwagi wprowadzające do Rozdziału XXXIII Kodeksu karnego „Przestępstwa przeciwko ochronie informacji"* (w:) G. Bogdan, K. Buchała, Z. Ćwiąkalski, M. Dąbrowska-Kardas, P. Kardas, J. Majewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel, A. Zoll, *Kodeks karny. Część szczególna. Komentarz*, t. 2, Kraków–Zakamycze 1999, s. 968–969.

[3] Zob. szerzej R. Skubisz, *Internet...*, s. 11; R. Warner, *Web Contracting* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 125–140; G. Wiaderek, *Internetowe czynności bankowe a forma pisemna czynności prawnych* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 141–150; M. Chajda, *Prowadzenie działalności bankowej z wykorzystaniem systemów informatycznych* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 151–161; T. Obal, *Wpływ bankowości elektronicznej na ryzyko bankowe*, Bezpieczny Bank 1998, nr 4, s. 85–91; M. Kondrat, *Handel elektroniczny — regulacje europejskie* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 171–184; J. Pobierajło, *Bankowość elektroniczna*, Bank 1999, nr 5, s. 49–54.

[4] Zob. szerzej S. Stanisławska-Kloc, *Przedmiot prawa autorskiego...*, s. 15 i n.

[5] M. Safjan, *Ochrona danych osobowych — granice autonomii informacyjnej. Paradoks towarzyszący rozwojowi współczesnych technik informatycznych* (w:) *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 11–12.

wia, że informacja uzyskuje niezwykłą wartość, w wielu przypadkach zaś staje się towarem, takim samym jak wszelkie inne towary mające materialną postać. Zasoby informacyjne stanowią dobro o dużej wartości ekonomicznej w sferze działalności gospodarczej,[6] są niezwykle istotnym instrumentem w sferze polityki i władzy publicznej,[7] decydującym często o efektywnym sprawowaniu władzy politycznej;[8] stanowią istotny element skutecznego stosowania procedur kontroli społecznej.[9] Zarazem jednak informacja, uzyskując status dobra o istotnej wartości społecznej, tym samym narażona jest na różnego rodzaju ataki i manipulacje, których celem jest uzyskanie przewagi in-

[6] Na ten element informacji zwraca uwagę A. Bierć, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce — aspekty cywilnoprawne. Przesłanki oraz środki prawne ochrony danych osobowych przedsiębiorcy i konsumenta* (w:) *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 111 i n. Truizmem wręcz będzie stwierdzenie, że systematycznie wzrasta rola wykorzystywania nowoczesnych technologii gromadzenia, przetwarzania i przesyłania danych w sferze gospodarki. Zdematerializowany został w dużym stopniu obrót papierami wartościowymi, w coraz szerszym zakresie Internet wykorzystywany jest do działalności handlowej (tzw. sklepy internetowe) oraz publicystycznej, staje się istotnym środkiem komunikacji społecznej. Zob. szerzej K.J. Jakubski, *Przestępczość komputerowa — próba zdefiniowania zjawiska* (w:) *Internet — problemy prawne*, red. R. Skubisz, Lublin 1999, s. 281; J. Preussner-Zamorska, *Zakres prawnie chronionej tajemnicy w postępowaniu cywilnym*, Kwartalnik Prawa Prywatnego 1998, z. 2, s. 287 i n.; S. Sołtysiński (w:) S. Sołtysiński, A. Szwaja (red.), A. Szajkowski, *Ustawa o zwalczaniu nieuczciwej konkurencji*, Warszawa 1994, s. 97 i n.; R. Zakrzewski, *Ochrona informacji w nowym kodeksie karnym*, Przegląd Ustawodawstwa Gospodarczego 1998, Nr 10, s. 10 i n.; R.P. Skiba, *Tajemnica bankowa a ochrona danych osobowych*, Biuletyn Bankowy 2000, nr 2, s. 1 i n.

[7] Jak podkreśla W. Cwalina, „głównym motorem rewolucji informacyjnej lat 90-tych jest Internet. (...) Nic więc dziwnego, że potencjał Internetu został także dostrzeżony przez polityków. Większość agend rządowych na całym świecie posiada własne strony internetowe (...). Coraz częściej pojawiają się również próby wykorzystywania łączy elektronicznych w celu włączenia społeczności lokalnych w procesy sprawowania władzy. Wyraźnie podkreślane są także możliwości Internetu w dyplomacji (...). Jednak najbardziej obiecujące i zdobywające coraz większą popularność jest użycie Internetu jako kolejnego z narzędzi marketingu politycznego" (*Marketing...*, s. 312–313). Zob. też A. Pawłowska, *Władza...*, s. 35 i n.

[8] Trafnie wskazuje M. Safjan, że „człowiek zawsze dążył do władzy i kontroli nad informacją" czyniąc zasoby informacyjne niezwykle skutecznym instrumentem walki politycznej (*Ochrona danych...*), s. 9 i n. Podobnie zagadnienie to ujmuje W. Wróbel, *Uwagi wprowadzające...*, s. 968 i n.

[9] O wzajemnych relacjach procesowego prawa karnego i regulacji prawnych odnoszących się do nowoczesnych technik gromadzenia i przetwarzania informacji w kontekście jurydycznych formuł służących ochronie informacji piszą szeroko: R. Hamm, *Ochrona danych osobowych a prawo karne* (w:) *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 73 i n.; S. Ziółkowski, *Nowoczesne technologie przetwarzania informacji a projektowane zmiany procedury karnej* (w:) *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, red. A. Adamski, Toruń 1994, s. 193 i n. oraz W. Kulesza, *Ochrona danych osobowych a nowa kodyfikacja prawa karnego w Polsce* (w:) *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 89 i n.; R. Kmiecik, *Prawnodowodowe aspekty ochrony programów komputerowych w postępowaniu karnym (problematyka wszczęcia postępowania)*, Prokuratura i Prawo 1997, nr 6, s. 7 i n.

formacyjnej środkami nie zawsze dozwolonymi, stwarzającej przesłanki do zdobycia lub utrzymania władzy politycznej, uzyskania lub utrzymania przewagi ekonomicznej czy też uzyskania odpowiedniej efektywności procedur kontroli społecznej, która przejawia się m.in. w stworzeniu specjalnych procedur dowodowych,[10] ograniczeniu prawa oskarżonego do ochrony informacji[11] lub ograniczeniu zakresu ochrony tajemnicy w postępowaniu cywilnym.[12] Możliwość dokonywania różnego rodzaju nadużyć w sferze automatycznego gromadzenia i przetwarzania zasobów informacyjnych jest tym większa, że korzystając ze zdobyczy nowoczesnej technologii informacje można przetwarzać, powielać, kompilować, przeszukiwać, przesyłać, rozpowszechniać i modyfikować z niezwykłą szybkością i dokładnością. Co więcej, wszystkie wymienione wyżej jedynie przykładowo działania, jakie dokonywane być mogą na zasobach informacyjnych, ze względu na wykorzystywanie nowoczesnych technologii cyfrowych charakteryzują się tak daleko idącą specyfiką, iż nie sposób do ich regulacji wykorzystywać tradycyjnych konstrukcji prawnych.[13] Nowoczesne metody gromadzenia i przetwarzania danych wymykają się więc tradycyjnym metodom kontroli i przyjmowanym w tradycyjnych ustawodawstwach sposobom regulacji, służącym zapewnieniu bezpieczeństwa i ochrony

[10] W piśmiennictwie wskazuje się na potrzebę szybkiego uregulowania zagadnień dotyczących sposobów pozyskiwania i zabezpieczenia dowodów związanych z działalnością opartą na nowoczesnych technologiach informatycznych. Zob. szerzej J. Dzierżanowska, M. Wąsek–Wiaderek, *Prawo karne a Internet — wybrane zagadnienia* (w:) *Internet — problemy prawne*, red. R. Skubisz, Lublin 1999, s. 259–260; K.J. Jakubski, *Przestępczość komputerowa...*, s. 283 i n.

[11] Zob. szerzej R. Hamm, *Ochrona danych...*, s. 80–81; S. Ziółkowski, *Nowoczesne technologie...*, s. 195 i n.; K. Dudka, *Podsłuch komputerowy w polskim procesie karnym — wybrane zagadnienia*, Prokuratura i Prawo 1999, nr 1, s. 69 i n.; tejże, *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998, s. 10 i n.; tejże, *Zatrzymanie korespondencji w projekcie kodeksu postępowania karnego z 1995 r. na tle przepisów obowiązujących*, Prokuratura i Prawo 1996, Nr 4, s. 26 i n.; B. Kurzępa, *Kontrola i utrwalanie rozmów telefonicznych według kodeksu postępowania karnego*, Prokuratura i Prawo 1999, nr 3, s. 77 i n.

[12] Zob. szerzej J. Preussner–Zamorska, *Zakres...*, s. 287 i n.

[13] Zob. szerzej w tej kwestii J. Barta, R. Markiewicz, *Główne problemy prawa komputerowego*, Warszawa 1993, s. 23 i n.; A. Nowacka, *Prawnoautorska i patentowa ochrona programów komputerowych*, Warszawa 1995, s. 12 i n.; J. Barta, R. Markiewicz, *Internet a prawo...*, s. 11 i n.; K. Golat, R. Golat, *Prawo komputerowe — zagadnienia podstawowe*, Warszawa 1998, s. 22 i n.; A. Adamski, *Przestępstwa komputerowe w nowym kodeksie karnym. Nowa kodyfikacja karna. Kodeks karny. Krótkie komentarze*, z. 17, Ministerstwo Sprawiedliwości. Departament Kadr i Szkolenia, Warszawa 1998, s. 9 i n.; K. Paradowski, *Metody zabezpieczenia danych z komputerowych nośników informacji* (w:) *Internet — problemy prawne*, red. R. Skubisz, Lublin 1999, s. 35 i n.; M. Skórzewska–Amberg, *Ochrona prawna danych i systemów komputerowych — wybrane zagadnienia* (w:) *Materiały konferencyjne InterSec'96*, s. 18 i n.; J. Dzierżanowska, *Karnoprocesowa problematyka przestępczości komputerowej* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 286–296.

danych.[14] Wraz ze wzrostem liczby podmiotów uzyskujących dostęp do cybernetycznych systemów gromadzących i przetwarzających informacje, których symbolem jest obecnie sieć internetowa umożliwiająca praktycznie każdemu dostęp do informacji oraz możliwość jej kreatywnego kształtowania,[15] pojawia się coraz więcej pól potencjalnych konfliktów,[16] u podłoża których leży dostępność do źródeł informacji, a także możliwość ich wykorzystywania oraz wpływania na ich kształt. W zależności od sfery społecznej, w jakiej określonego rodzaju informacje są gromadzone i wykorzystywane, możliwe jest występowanie owych konfliktów na różnych piętrach i poziomach. W obszarze relacji jednostka–państwo spostrzec można przesłanki istnienia konfliktu wertykalnego między jednostką (interesem prywatnym) a państwem (interesem publicznym), w obszarze relacji podmiot–podmiot możliwy jest konflikt horyzontalny pomiędzy poszczególnymi jednostkami, i to zarówno takimi, które zajmują się prowadzeniem działalności gospodarczej, jak i takimi, które nie pozostają w żadnych, poza konsumenckimi,[17] relacjach z wyspecja-

[14] O nieadekwatności tradycyjnych instrumentów prawnych do realiów społeczeństwa informatycznego piszą szeroko na przykładzie Internetu J. Barta i R. Markiewicz (*Internet a prawo..., passim*, oraz *Główne problemy..., passim*). Zob. też K. Buchała, *Computer Crimes and Other Crimes against Information Technology in Poland* (w:) *Ius Informationis. European Series on Information Law, volume 6, Information Technology Crime. National Legislations and International Initiatives*, ed. U. Sieber, Würzburg 1994, s. 377 i n.; U. Sieber, *Przestępczość komputerowa...*, s. 223 i n.; tenże, *Informationstechnologie und Strafrechtsreform*, Berlin 1985, s. 23 i n.; K. Tiedemann, *Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber*, Juristenzeitung 1986, s. 865 i n.; L. Bühler, *Ein Versuch, Computerkriminellen das Handwerk zu legen, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität*, Monatsschrift für deutsches Recht 1987, s. 448; K.J. Jakubski, *Przestępczość komputerowa i jej ściganie — wybrane zagadnienia* (w:) *Materiały konferencyjne InterSec'96*, s. 28 i n.; E. Buduj, *Fałszerstwa dokumentów stanowiących wydruki komputerowe* (w:) *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, red. A. Adamski, Toruń 1994, s. 64 i n.; B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno–kryminalistyczne*, Kraków–Zakamycze 1999, s. 172 i n.

[15] Posługując się sformułowaniem „możliwość kreatywnego przekształcania informacji", mam na myśli przede wszystkim dostępną dla każdego użytkownika Internetu (internauty) możliwość dowolnej segregacji, łączenia, kompilowania, rozdzielania itp. różnego rodzaju informacji zgromadzonych w dostępnych bazach danych. Podkreślić należy, iż z uwagi na globalny charakter Internetu jego użytkownicy mają dostęp do informacji zgromadzonych w bazach na całym świecie. Szerzej o interaktywności Internetu pisze M. Majewski, *Interaktywność Internetu* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 297–308. W kwestii wzajemnych relacji regulacji prawnych i Internetu zob. szerzej J. Barta, R. Markiewicz, *Internet a prawo...*, s. 28 i n.

[16] W pierwszej kolejności wskazać należy na konflikty między dysponentami baz danych a podmiotami, których dotyczą zgromadzone tam informacje. Zob. szerzej A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 25 i n.

[17] O znaczeniu istnienia szczególnych regulacji prawnych dotyczących gromadzenia i przetwarzania danych w sferze obrotu konsumenckiego pisze B. Fischer, *Gospodarka elektroniczna*, Prawo i Życie 2000, nr 1, s. 58–63.

lizowanym obrotem gospodarczym. Wreszcie nie sposób wykluczyć konfliktu czystych praw podmiotowych: pomiędzy prawem do prywatności a prawem do informacji.[18] Informacja stając się wartością rynkową wymusza tym samym stworzenie odpowiednich prawnych regulacji, które określałyby sposoby jej wykorzystywania przy zastosowaniu nowoczesnych technologii. Dokonująca się lawinowo komputeryzacja, która oznacza jakościowe zmiany w procesach gromadzenia i przekazywania informacji, rodzi nowe problemy związane z jej prawną ochroną, zaś brak całościowej i zupełnej regulacji prawnej w tej sferze stwarza trudne do wyobrażenia możliwości nadużyć i w istocie hamuje rozwój racjonalnej gospodarki komputerowej.[19] W powyższym kontekście jako oczywista jawi się konieczność wypracowania takich rozwiązań prawnych, aby stworzyć podstawy zapewnienia odpowiedniej równowagi między ochroną interesu jednostek, których dotyczą gromadzone i przetwarzane dane (prawem do prywatności) a swobodą przepływu tych danych w społeczeństwie (prawo do informacji), przy założeniu, że poszczególne podmioty bardzo często występują w różnych rolach społecznych, niejednokrotnie przeciwstawnych.[20] Konieczność wprowadzenia zmian w wewnętrznym porządku prawnym oraz potrzeba stworzenia nowych regulacji prawnych, dostosowanych do wymogów współczesnego świata były wielokrotnie przedmiotem raportów oraz różnego rodzaju rezolucji i uchwał organizacji ponadnarodowych.[21]

[18] Identyczną typologię możliwych konfliktów przedstawia M. Safjan, *Ochrona danych*..., s. 9–11. Zob. też W. Wróbel, *Uwagi wprowadzające*..., s. 969–970; M. Safjan, *Prawo do ochrony życia prywatnego* (w:) *Podstawowe prawa jednostki i ich sądowa ochrona*, red. L. Wiśniewski, Warszawa 1997, s. 127 i n.; P. Hofmański, *Konwencja europejska a prawo karne*, Toruń 1995, s. 21 i n. oraz s. 319 i n.; tenże, *Prawo do poszanowania prywatności (art. 17 Paktu i art. 8 Europejskiej Konwencji Praw Człowieka) a rozwiązania polskiego prawa karnego materialnego i procesowego* (w:) *Standardy praw człowieka a polskie prawo karne*, red. J. Skupiński, J. Jakubowska–Hara, Warszawa 1995, s. 253 i n.; M.A. Nowicki, *Europejska Konwencja Praw Człowieka. Wybór orzecznictwa*, wyd. 2, Warszawa 1999, s. 327–386 i 570–572.

[19] Por. K. Dudka, *Podsłuch komputerowy*..., s. 69.

[20] Zob. A. Bieć, *Ochrona prawna*..., s. 111.

[21] Zagadnienie wykorzystywania nowoczesnych technologii cyfrowych dla gromadzenia, przetwarzania i przesyłania informacji oraz problem tzw. przestępstw komputerowych (a więc pewien fragment problematyki związanej z nowoczesnymi technologiami w sferze gromadzenia i przetwarzania danych) było w latach 80–tych przedmiotem licznych raportów, zaleceń i rezolucji kierowanych do rządów poszczególnych państw przez organizacje międzynarodowe takie, jak: OECD, Rada Europy, Zgromadzenie Ogólne Narodów Zjednoczonych. Konkretne postulaty rozwiązań prawnych zawierają m.in. Konwencja Nr 108 z dnia 28 stycznia 1981 r. dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych oraz Dyrektywa Nr 95/46/CE w sprawie ochrony osób fizycznych ze względu na przetwarzanie danych o charakterze osobowym oraz swobodnego przepływu tych danych, rekomendacja Komitetu Ministrów Rady Europy Nr R (89) 9 w sprawie przestępstw komputerowych, Zalecenie Nr R (95) 13 Komitetu Ministrów Rady Europy dotyczące problemów przepisów postępowania karnego związanych z technologią informatyczną oraz załącznik do Zalecenia Nr R (95) 13 odnoszący się do problematyki dowodowej związanej z technologią informatyczną; Dyrektywa Unii Europejskiej Nr 95/46/CE z 24 października 1995 r. w sprawie ochrony osób fizycznych ze względu na przetwarzanie danych o charakterze osobowym oraz swobodnego przepływu tych danych. Zob. szerzej A. Adamski, *Przestępstwa komputerowe*..., s. 9, zwłaszcza przypis nr 3; tenże, *Prawo karne komputerowe*..., s. 219–263; A. Mednis, *Ochrona danych osobowych w konwencji rady Europy i dyrektywie Unii Europejskiej*, Państwo i Prawo 1997, nr 6, s. 26 i n.; tenże, *Prawna ochrona danych osobowych*, Warszawa 1995, s. 16 i n.; P. Hofmański, *Konwencja europejska*..., s. 319 i n.; S. Redo, *Prevention and control of computer crime from the United Nations perspective* (w:) *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, red. A. Adamski, Toruń 1994, s. 71 i n.; B. Fischer, *Przestępstwa komputerowe*..., s. 237–245 (autor ten w Aneksie opracowania zamieszcza polski tekst Zalecenia Nr R (89) 9 i Zalecenia Nr R (95) 13 wraz z załącznikiem); J. Dzierżanowska, M. Wąsek–Wiaderek, *Prawo karne a Internet*..., s. 257–258; K.J. Jakubski, *Przestępczość komputerowa*..., s. 266 i n.

2. Wprowadzenie do systemu prawa wewnętrznego prawnych regulacji, które służyłyby ochronie informacji gromadzonych w nowoczesnych systemach komputerowych może przybierać różne formy prawne wykorzystujące tradycyjne mechanizmy wypracowane w poszczególnych dziedzinach prawa. Skuteczne instrumenty ochrony można budować, wykorzystując jako podstawę regulacji konstrukcje cywilistyczne, prawnoautorskie, prawnoadministracyjne oraz prawnokarne. Model regulacji, w tym zwłaszcza powiązanie go z instrumentami charakterystycznymi dla danej dziedziny prawa, uzależniony jest od charakteru operacji mających podlegać ochronie, a dokonywanych na komputerowych bazach danych, od istoty praw związanych z informacjami zawartymi w tych bazach, wreszcie od zakresu i rodzaju niebezpieczeństw związanych z niedozwolonymi zamachami na te bazy.[22] Niezależnie od obranej przez ustawodawcę normatywnej formy ochrony, w pewnym zakresie konieczne jest jednak uzupełnienie jej regulacjami właściwymi dla prawa karnego. Część zjawisk patologicznych występujących w obszarze cybernetycznego gromadzenia, przetwarzania i przesyłania informacji charakteryzuje się tak wysoką społeczną szkodliwością, iż wprowadzenie w tym obszarze kryminalizacji jest w pełni uzasadnione.[23] Zagrożenie karą krymi-

[22] Wskazanie na wielość działów prawa, w których możliwe jest wprowadzenie specjalnych regulacji odnoszących się do cyfrowych technologii gromadzenia i przetwarzania danych pozostaje w związku z prezentowanymi w piśmiennictwie poglądami, wedle których wprowadzanie nowych rozwiązań prawnych odnoszących się do cyberprzestrzeni uwzględniać musi tradycyjne zasady prawa oraz prowadzić do modyfikacji istniejącego stanu prawnego tylko w takim zakresie, w jakim jest to niezbędne. Zob. też R. Skubisz, *Internet*..., s. 13.

[23] Co do społecznej szkodliwości poszczególnych kategorii zachowań jako konstytucyjnej przesłanki wprowadzenia karalności zob. szerzej: M. Dąbrowska–Kardas, *O dwóch znaczeniach pojęcia społecznego niebezpieczeństwa czynu*, Czasopismo Prawa Karnego i Nauk Penalnych 1997, nr 1, s. 19–38; A. Zoll, *Nowa kodyfikacja karna w świetle Konstytucji*, Czasopismo Prawa Karnego i Nauk Penalnych 1997, nr 2, s. 97–110; tenże, *Zasady prawa karnego w projekcie Konstytucji*, Państwo i Prawo 1997, nr 3, s. 72 i n.; tenże, *Materialne określenie przestępstwa*, Prokuratura i Prawo 1997, nr 2, s. 7 i n.; L. Gardocki, *Zagadnienia teorii kryminalizacji*, Warszawa 1990, s. 66 i n.

nalną pewnej kategorii przekroczeń, dokonywanych w sferze gromadzenia i przetwarzania informacji przy wykorzystaniu nowoczesnych technologii cyfrowych, służyć ma, z jednej strony, wzmocnieniu uregulowań właściwych dla danej sfery prawa, z drugiej zaś — stwarzać instrumenty prawne pozwalające na stosowanie sankcji karnej tam, gdzie mechanizmy charakterystyczne dla innych dziedzin prawa nie są wystarczające.[24] W tej perspektywie, także w sferze nadużyć związanych z wykorzystywaniem nowoczesnych technologii cyfrowych, prawo karne jawi się jako *ultima ratio*,[25] instrument, który wspomagać ma regulacje zawarte w innych działach prawa.[26] Konstrukcje prawnokarne, które służą kryminalizacji bezprawnych zachowań godzących w informacje gromadzone, przetwarzane i przesyłane za pomocą nowoczesnych technologii cyfrowych określa się czasami mianem „przestępczości komputerowej".[27] Aby jednak prawidłowo postrzegać istotę prawnokarnych regulacji odnoszących się do przestępczości komputerowej, nie sposób pominąć kilku kwestii związanych z genezą tej specyficznej sfery zachowań podlegających karze oraz jej związków z rozwiązaniami przyjmowanymi w innych działach prawa.

[24] Zob. A. Adamski, *Karalność hackingu na podstawie przepisów kodeksu karnego z 1997 r.*, Przegląd Sądowy 1998, nr 11–12, s. 149 i n.

[25] Identycznie zagadnienie to ujmują J. Dzierżanowska, M. Wąsek–Wiaderek, *Prawo karne a Internet...*, s. 239.

[26] Co do zasady subsydiarności prawa karnego zob. szerzej: K. Buchała, A. Zoll, *Polskie prawo karne*, Warszawa 1995, s. 14 i n.; A. Marek, *Prawo karne. Zagadnienia teorii i praktyki*, Warszawa 2000, s. 14 i n. A. Zoll, *O normie prawnej z punktu widzenia prawa karnego*, Krakowskie Studia Prawnicze 1990, s. 69 i n.; tenże, *Zasady prawa karnego w projekcie Konstytucji*, Państwo i Prawo 1997, nr 3, s. 35 i n.; H.–H. Jescheck, T. Weigend, *Lehrbuch des Strafrechts. Allgemeiner Teil*, 5. Auflage, Berlin 1996, s. 52–54; A. Kaufmann, *Subsidiaritätsprinzip und Strafrecht* (w:) *Festschrift für H. Henkel*, Berlin 1974, s. 89 i n.; tenże, *Tendenzen im Rechtsdenken der Gegenwart*, München 1976, *passim*; W. Küper, *Die „Sache mit den Tieren"*, Juristenzeitung 1993, s. 435 i n.; W. Maiwald, *Zum fragmentarischen Charakter des Strafrechts* (w:) *Festschrift für R. Maurach*, Berlin 1972, s. 9 i n.

[27] Pojęcie „przestępczość komputerowa" lub „przestępstwa komputerowe" nie ma jednak, jak dotąd, w miarę precyzyjnie oznaczonego zakresu znaczeniowego i wykorzystywane jest, w zależności od potrzeb, dla określania różnorodnych przejawów przestępczości powiązanych z nowoczesnymi technologiami gromadzenia i przetwarzania danych. Kwestia zakresu znaczeniowego tego pojęcia i jego roli w analizach dogmatycznych będzie przedmiotem rozważań w dalszej części niniejszego opracowania. Zob. szerzej K.J. Jakubski, *Przestępczość komputerowa — zarys problematyki*, Prokuratura i Prawo 1996, nr 12, s. 34 i n.; tenże, *Przestępczość komputerowa...*, s. 263 i n.; A. Adamski, *Przestępstwa komputerowe...*, s. 15 i n.; tenże, *Prawo karne komputerowe...*, s. 30 i n.; W. Jasiński, *Wykorzystanie elektronicznych przelewów funduszy do prania pieniędzy*, Prokuratura i Prawo 1998, nr 4, s. 57 i n.; R. Kmiecik, *Prawnodowodowe aspekty...*, s. 7 i n.

II. GENEZA TZW. PRZESTĘPCZOŚCI KOMPUTEROWEJ

3. Punktem wyjścia w procesie dostosowywania regulacji prawnych do wymogów społeczeństwa informacyjnego były wprowadzane w wielu krajach na początku lat siedemdziesiątych szczególne rozwiązania, mające na celu ochronę danych osobowych gromadzonych na komputerowych nośnikach informacji.[28] Dane osobowe (innymi słowy — informacje dotyczące podmiotu) jako pierwsze doczekały się więc wyspecjalizowanej reakcji ustawodawcy w postaci wyodrębnionych aktów prawnych zawierających kompleksowe regulacje, mające na celu zapewnienie bezpieczeństwa bazom danych osobowych zgromadzonych na elektronicznych nośnikach.[29] Już w 1970 r. uchwalona została pierwsza ustawa o ochronie danych osobowych w Hesji,[30] w roku 1973 Szwecja wprowadziła specjalną ustawę służącą ochronie danych osobowych przed zagrożeniami płynącymi z możliwości wykorzystywania nowoczesnych technologii.[31] W krótkim okresie wzorzec niemiecki i skandynawski został wykorzystany w regulacjach wielu krajów świata,[32] w tym także — ponad dwadzieścia lat później — w Polsce.[33]

[28] W piśmiennictwie wskazuje się, że rzeczywiste początki tzw. przestępczości komputerowej sięgają pierwszej połowy lat pięćdziesiątych, tj. okresu pojawienia się na amerykańskim rynku komputerów tzw. drugiej generacji. Upowszechnienie się tej specyficznej kategorii przestępstw nastąpiło jednak kilkanaście lat później, gdy pojawiły się powszechnie dostępne komputery tzw. trzeciej generacji. Zob. szerzej S. Frey, *Computerkriminalität in eigentums- und vermögensstrafrechtlicher Sicht*, München 1987, s. 5 i n.; W. Rupp, *Computersoftware und Strafrecht. Ein Beitrag unter besonderer Berücksichtigung des sttrafrechtlichen Vermögensschutzes*, Tübingen 1985, s. 29 i n.; T. Lenckner, *Computerkriminalität und Vermögensdelikte,* Heidelberg–Karlsruhe 1981, s. 19 i n.; A. Adamski, *Prawo karne komputerowe...*, s. 1 i n.; R. Czachowski, P. Sienkiewicz, *Przestępcze oblicza komputerów...*, s. 53–54; K.J. Jakubski, *Przestępczość komputerowa...*, s. 263 i n.; M. Kolecki, *Przestępstwa komputerowe w ustawodawstwie federalnym Stanów Zjednoczonych A.P.*, Palestra 1992, nr 4, s. 52 i n.

[29] Zob. szerzej A. Mednis, *Prawna ochrona...*, Warszawa 1995, s. 12 i n.

[30] Zob. U. Sieber, *Przestępczość komputerowa...*, s. 232 i n.

[31] Zob. szerzej w tej kwestii J. Michael, *Privacy and Human Rights. An International and Comparative Study with Special Reference to Developments in Information Technology*, UNESCO Publishing, Darmouth 1994, s. 3 i n.; A. Adamski, *Przestępstwa komputerowe...*, s. 9.

[32] Szczególne ustawy dotyczące problematyki ochrony danych osobowych posiadają m.in., Dania, Francja, Norwegia, Austria (wszystkie uchwalone w 1978), Luksemburg, Islandia, Izrael (pochodzące z 1981 r.), Wielka Brytania (1984), Kanada (1985), Finlandia (1987), Irlandia, Japonia, Holandia (1988), Portugalia (1991), Belgia, Szwajcaria, Hiszpania, Słowacja, Czechy, Węgry (1992 r.); zob. B. Fischer, *Przestępstwa komputerowe...*, s. 174; U. Sieber, *Przestępczość komputerowa...*, s. 20 i n.

[33] Zagadnienie ochrony danych osobowych reguluje kompleksowo ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r. Nr 133, poz. 883). Zob. szerzej: A. Mednis, *Ustawa...*, s. 7 i n.; A. Adamski, *Prawo karne komputerowe...*, s. 1411 i n.

Obok samej ochrony danych osobowych, wkrótce pojawił się problem innego rodzaju nadużyć popełnianych z wykorzystaniem systemów komputerowych. Automatyzacja gromadzenia i przetwarzania danych dokonywana przy pomocy nowoczesnych systemów komputerowych, w tym zwłaszcza danych i informacji niezbędnych dla prawidłowego funkcjonowania obrotu gospodarczego, stworzyła niezwykłe wręcz możliwości nadużyć za pośrednictwem tych systemów. Szczególnym przedmiotem zainteresowania stały się w tym obszarze tego rodzaju dane i informacje, które stanowiły odzwierciedlenie określonych praw majątkowych lub niemajątkowych. Nowoczesna formuła ataku skierowanego na dobra materialne (majątkowe), wyrażone w postaci niematerialnej przyjmującej formę zapisu cyfrowego na odpowiednim nośniku informacji, okazała się na tyle atrakcyjna, że znaczna część zachowań patologicznych, wymierzonych w określone wartości, przybrała nową postać polegającą na wykorzystywaniu nowoczesnych technologii związanych z komputerowym gromadzeniem, przekształcaniem i przekazywaniem danych. Wiele klasycznych rodzajów zamachów na prawa majątkowe od chwili upowszechnienia komputerowych systemów gromadzących, przetwarzających i przesyłających dane zastąpionych zostało wyrafinowanymi technikami ataków na dobro prawne, których dokonywano przy wykorzystaniu komputera. Obok tego zamachy skierowano na same bazy danych i informacje zgromadzone w odpowiednich systemach, ponieważ także one stanowić zaczęły wartość — po pierwsze, z tego powodu, iż z określonymi zapisami cyfrowymi połączone były bezpośrednio prawa o charakterze majątkowym, po drugie — gdyż samo bezawaryjne funkcjonowanie systemu informatycznego w wielu sferach stało się autonomiczną wartością. Wszelkie formy zamachów dokonywanych przy wykorzystaniu nowych technik gromadzenia i przetwarzania danych, zarówno te skierowane na dobra wyrażane jedynie poprzez odpowiednie zapisy w systemie, jak i te godzące jedynie w sam system, z ogromnym trudem pozwalały się kwalifikować na podstawie tradycyjnych instytucji prawnej ochrony.[34] Stąd też już na początku lat osiemdziesiątych zaczęto wprowadzać nowe regulacje prawne, dostosowane do nowoczesnych form ataków na dobra prawne dokonywanych z pomocą nowoczesnych technik cybernetycznych.[35] Wiele krajów wprowadziło specjalne przepisy służące zwalczaniu przestępczości związanej z wykorzystaniem komputerów o charakterze ekonomicznym.[36]

[34] Zob. szerzej F. Haft, *Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (Computerdelikte)*, Neue Zeitschrift für Strafrecht, 1987, s. 6 i n.; K. Leicht, *Computerspionage — Die „besondere Sicherung gegen ungerechtigten Zugang" (§ 202a StGB)*, Informatik und Recht 1987, s. 45 i n.; P. Cramer (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar*, 25., Neubearbeitete Auflage von T. Lenckner, P. Cramer, A. Eser, W. Stree, München 1998, s. 1755–1765; R. Engelhard, *Computerkriminalität und deren Bekämpfung durch strafrechtliche Reformen*, Datenverarbeitung im Recht 1985, s. 165 i n.; K. Lampe, *Die strafrechtliche Behandlung der sog. Computerkriminalität*, Goltdammer's Archiv für Strafrecht 1975, s. 1 i n.

Ostatnim etapem rozwoju szczególnego ustawodawstwa związanego z ochroną informacji w nowoczesnych systemach cybernetycznych było wprowadzenie specjalnych reguł prawnych, które zwiększały ochronę samych programów obsługujących nowoczesne systemy informatyczne oraz programów wykorzystywanych w komputerach i systemach komputerowych. Najpierw, w latach siedemdziesiątych, konstrukcje prawne chroniące programy komputerowe tworzono z wykorzystaniem modelu ochrony patentowej.[37] Później, uznając nieskuteczność tego modelu, modyfikowano system prawnej ochrony poprzez objęcie programów komputerowych zakresem prawa autorskiego.[38]

Wreszcie całkiem już współcześnie, w latach dziewięćdziesiątych, pojawił się problem związany z ochroną danych i informacji wykorzystywanych w sieciach informatycznych. Naruszanie różnego rodzaju dóbr, w tym także dobra, jakim jest informacja, zaczęło następować poprzez systemy i sieci komputerowe, sieci teleinformatyczne (np. Internet).[39] Internet — w założeniu instrument służący do nieograniczonego wręcz przekazywania różnorodnych informacji — stał się jednocześnie źródłem niespotykanych dotąd zagrożeń dla jego użytkowników. Wykorzystując ten niezwykły środek komunikowania

[35] Regulacje prawnokarne służące ochronie obrotu gospodarczego przed zamachami dokonywanymi przy wykorzystaniu nowoczesnych technologii cyfrowych do tego stopnia zdominowały literaturę prawniczą, iż w pewnym okresie przestępstwa komputerowe utożsamiane były ze specjalną kategorią przestępstw gospodarczych. Tak np. S. Frey jeszcze w 1985 r. jeden z rozdziałów swojego opracowania poświęconego przestępstwom komputerowym zatytułowała *„Computerkriminalität als Teil der Wirtschaftskriminalität?"* (*Computerkriminalität in eigentums- und vermögensstrafrechtlicher Sicht*..., s. 10–15). Zob. też K. Tiedemann, *Erscheinungsformen der Wirtschaftskriminalität und Möglichkeiten ihrer strafrechtlichen Bekämpfung*, ZStW 1976, s. 231–260.

[36] Jak podaje A. Adamski, (*Przestępstwa komputerowe*..., s. 10), specjalne ustawy służące zwalczaniu komputerowej przestępczości o charakterze ekonomicznym wprowadziły jako pierwsze USA w 1976 r., następnie podobne rozwiązania przyjęto we Włoszech (1978), Wielkiej Brytanii (1981), Australii (1983), Kanadzie i Danii (1985), RFN, Szwecji i Chile (1986), Austrii, Japonii i Norwegii (1987) oraz Francji, NRD, Grecji (1988). Zob. też U. Sieber, *Przestępstwa komputerowe*..., s. 20 i n.; B. Fischer, *Przestępstwa komputerowe*..., s. 179 i n.

[37] Zob. A. Nowacka, *Prawnoautorska*..., s. 12 i n.; J. Barta, R. Markiewicz, *Główne problemy*..., s. 54 i n.; S. Sołtysiński (w:) *System prawa własności intelektualnej*, t. III, *Prawo wynalazcze*, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1990, s. 29 i n.

[38] Na tym modelu oparte są rozwiązania przyjęte w polskiej ustawie o prawie autorskim i prawach pokrewnych. Zob. szerzej A. Nowacka, *Prawnoautorska*..., s. 9 i n.

[39] Zob. szerzej: J. Barta, R. Markiewicz, *Internet a prawo*..., *passim*; J. Dzierżanowska, M. Wąsek-Wiaderek, *Prawo karne a Internet*..., s. 239 i n.; K.J. Jakubski, *Przestępczość komputerowa*..., s. 263 i n.

się, można w sposób praktycznie pozbawiony jakiejkolwiek kontroli rozpowszechniać informacje objęte ścisłymi zakazami, w swej istocie niedozwolone, takie jak np. treści pornograficzne, propagujące przemoc, poglądy rasistowskie itp.[40] Także ta sfera wykorzystywania nowoczesnych technologii cyfrowych wymaga w miarę szybkiego uregulowania.[41]

4. Przedstawione wyżej skrótowe uwagi dotyczące sfer i możliwości związanych z wykorzystywaniem nowoczesnych technologii cyfrowych do gromadzenia, przetwarzania i przesyłania informacji zdają się wskazywać, że stworzenie kompleksowych nowoczesnych regulacji prawnych, które określałyby reguły i zasady posługiwania się tymi technologiami, stanowi jedno z istotniejszych wyzwań współczesności.[42] Niezależnie od tego, z jaką gałęzią prawa mamy do czynienia, tradycyjne instrumentarium prawnicze okazuje się całkowicie nieprzydatne w konfrontacji z cybernetyczną rzeczywistością.[43] Powszechność zastosowania nowoczesnej techniki komputerowej we wszystkich dziedzinach życia sprawia, iż nowoczesne regulacje prawne związane ze statusem, ochroną oraz zasadami obrotu danymi muszą uzupełniać wszystkie tradycyjne działy prawa. Mając na względzie specyfikę unormowań związa-

[40] Zob. szerzej J. Dzierżanowska, M. Wąsek-Wiaderek, *Prawo karne a Internet...*, s. 240 i n.

[41] Zob. szerzej U. Sieber, *Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetze*, Computer und Recht 1998, s. 581 i n; *Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. Eine strafrechtsvergleichende Untersuchung*, red. U. Sieber, Bonn 1999; M. Maj, K. Silicki, *Klasyfikacja i terminologia incydentów naruszających bezpieczeństwo sieci* (w:) *Internet 2000. Prawo-ekonomia-kultura*, red. R. Skubisz, Lublin 2000, s. 239 i n.; K.J. Jakubski, *Wyłudzanie towarów i usług na podstawie numerów kart kredytowych przez Internet* (w:) *Internet 2000. Prawo-ekonomia-kultura*, red. R. Skubisz, Lublin 2000, s. 249 i n.

[42] Z uwagi na transgraniczny charakter zamachów skierowanych na cybernetyczne systemy informatyczne, konieczne jest nie tylko stworzenie odpowiednich prawnych podstaw ochrony w ustawodawstwie poszczególnych krajów, lecz także określenie wspólnego standardu międzynarodowego stanowiącego podstawę zwalczania tego rodzaju zamachów. Zob. szerzej J. Dzierżanowska, M. Wąsek-Wiaderek, *Prawo karne a Internet...*, s. 241 i n.; K. J. Jakubski, *Przestępczość komputerowa...*, s. 282 i n.; tenże, *Przestępczość komputerowa — zarys...*, s. 34 i n.

[43] Nieadekwatność tradycyjnych konstrukcji prawnych służących ochronie określonych dóbr w konfrontacji z zamachami dokonywanymi przy wykorzystaniu nowoczesnych technologii informacyjnych dobrze ukazuje podawany przez A. Adamskiego przykład z Hongkongu, który dotyczy nieuprawnionego dostępu do korespondencji elektronicznej znajdującej się w komputerze innej osoby. Sprawca przypadkowo wszedł w posiadanie zabezpieczającego hasła i posługując się nim uzyskał zawartą w komputerze informację. Ze względu na brak szczególnych przepisów regulujących tego rodzaju bezprawne uzyskanie informacji, sąd orzekający w sprawie przyjął konstrukcję kradzieży energii elektrycznej, uznając sprawcę za winnego popełnienia tego przestępstwa (zob. szerzej A. Adamski, *Przestępstwa komputerowe...*, s. 14). Podobnie na nieskuteczność tradycyjnych mechanizmów ochrony prywatności postrzeganej w kontekście ochrony danych osobowych wskazuje także M. Safjan (*Ochrona danych...*, s. 13).

nych z wykorzystywaniem nowoczesnych technologii cyfrowego przetwarzania informacji, w piśmiennictwie dostrzega się wręcz potrzebę stworzenia nowej dyscypliny prawniczej, której cechą charakterystyczną będzie to, że podstawowym punktem odniesienia stanie się w niej zagadnienie ochrony danych i informacji gromadzonych i przetwarzanych przy wykorzystaniu nowoczesnych technologii. Tę nową dyscyplinę prawniczą określa się jako „prawo informatyczne", „prawo komputerowe", „prawo informacyjne", „prawo technologii informacyjnych" lub „prawo ochrony informacji".[44] Niezależnie od tego, jaką konwencję terminologiczną przyjmie się dla zbiorczego określenia tej nowej dziedziny prawa,[45] jedna kwestia wydaje się nie budzić wśród prawników większych wątpliwości: celem stworzenia odpowiednich regulacji prawnych, dostosowanych do standardów obowiązujących w „świecie informacyjnym", jest zapewnienie informacji jako takiej statusu autonomicznego dobra prawnego,[46] zasługującego na co najmniej taką samą ochronę jak ta, którą prawo zapewnia dobrom o charakterze materialnym.[47] Z drugiej strony, z uwagi na ogólnoświatowy charakter zjawiska, regulacje prawne odnoszące się do sfery automatycznego gromadzenia, przetwarzania i przesyłania informacji

[44] Zob. szerzej: J. Barta, R. Markiewicz, *Główne problemy...*, s. 166 i n.; A. Adamski, *Przestępstwa komputerowe...*, s. 8; tenże, *Prawo karne komputerowe...*, s. 30 i n.; U. Sieber, *Przestępczość komputerowa i prawnokarna ochrona informacji w międzynarodowej społeczności informacji i ryzyka*, Przegląd Policyjny 1995, nr 3 (39), s. 17 i n.; K.-M. Betzl, *Computerkriminalität — viel Lärm um Nichts? Eine Richtigstellung*, DSWR 1971/72, nr 1, s. 475 i n.; E.-J. Lampe, *Die strafrechtliche Behandlung der sog. Computer-Kriminalität*, GA 1975, s. 1 i n.; W. Müller, *Aktuelle Probleme des § 263 a StGB*, Frankfurt am Main-Berlin-Bern-New York-Paris-Wien 1999, s. 17 i n.; S. Frey, *Computerkriminalität in eigentums- und vermögensstrafrechtlicher Sicht*, München 1987, s. 5 i n.; G. Dannecker, *Neuere Entwicklungen im Bereich der Computerkriminalität*, BB 1996, s. 1285 i n.

[45] Zagadnienia terminologiczne wydają się o tyle nie odgrywać decydującej roli, że — jak trafnie wskazują J. Barta i R. Markiewicz — poszukiwanie nazwy dla tego nowego działu prawa dokonywane jest nieco na wyrost. Zdaniem tych Autorów, „w istocie w całym systemie prawa nie istnieje wyodrębniona gałąź prawa (taka, jaką jest np. prawo cywilne czy prawo karne), mająca za przedmiot komputery oraz programy, nie istnieje też w tej materii wyodrębniony zespół norm prawnych" (*Główne problemy...*, s. 15).

[46] Trafnie podkreśla U. Sieber, że niematerialna ze swej natury informacja potrzebuje nadania jej statusu autonomicznego dobra prawnego, które zasługuje na taką samą ochronę jak materia i energia. Zob. szerzej na ten temat: U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, Przegląd Policyjny 1995, nr 3(39), s. 27 i n.; tenże, *Computerkriminalität und Informationsstrafrecht, Computer und Recht 1995*, s. 100 i n.; tenże, *Computerkriminalität und andere Delikte im Bereich der Informationstechnik*, ZStW 1992 (104), s. 697 i n.; tenże, *Informationstechnologie...*, s. 51 i n.; T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 135 i n.; W. Müller, *Aktuelle Probleme...*, s. 20 i n.; J. Dzierżanowska, M. Wąsek-Wiaderek, *Prawo karne a Internet...*, s. 252 i n.

[47] Takie stanowisko prezentują także m.in. J. Barta, R. Markiewicz, *Główne problemy...*, s. 25 i n.; A. Adamski, *Przestępstwa komputerowe...*, s. 8 i n.; tenże, *Prawo karne komputerowe...*, s. 24 i n.; W. Wróbel, *Przestępstwa...*, s. 968 i n.

wymagają stworzenia ponadnarodowego standardu w zakresie regulacji tych kwestii, w tym zwłaszcza w sferze penalizacji określonych zjawisk.[48]

Regulacje dotyczące sfery nowoczesnych technologii gromadzenia, przetwarzania i przekazywania danych powinny z oczywistych powodów uzupełniać wszystkie tradycyjnie wyodrębniane w dogmatyce dziedziny prawa. Jednak szczególne znaczenie mają te obszary regulacji prawnej, które odnoszą się bezpośrednio do ochrony informacji jako dobra prawnego, służąc stworzeniu ram prawnych, wewnątrz których dokonywać się może legalny obrót danymi i informacją. W tym kontekście cztery sfery wydają się mieć szczególne znaczenie, a mianowicie: sfera konstytucyjnych podstaw ochrony informacji i danych osobowych w kontekście nowoczesnych technik gromadzenia i przetwarzania danych, sfera cywilistycznej ochrony prywatności w kontekście ochrony danych osobowych i informacji,[49] sfera ochrony baz danych oraz programów komputerowych i twórczości komputerowej, jako szczególnego przedmiotu prawa autorskiego,[50] i wreszcie najistotniejsza z punktu widzenia niniejszych rozważań sfera prawa karnego, związana z ochroną informacji i danych osobowych oraz kryminalizacją zamachów dokonywanych przy wykorzystaniu nowoczesnych technologii gromadzenia, przetwarzania i przesyłania informacji.

5. Wszystkie wymienione wyżej obszary, w jakich dochodzić może do naruszeń prawa do informacji oraz zasad jej wykorzystywania, zostały objęte szczególną regulacją przez polskiego ustawodawcę. Specjalną ochronę zapewnia się w polskim systemie prawnym danym osobowym, bazom danych, programom komputerowym oraz twórczości komputerowej; wreszcie stworzone zostały specjalne regulacje stanowiące podstawę karnoprawnej ochrony

[48] Takie stanowisko zajmują również U. Sieber, *Przestępczość komputerowa i prawnokarna ochrona prawa do informacji w międzynarodowej społeczności informacji i ryzyka*..., s. 224 i n.; J. Dzierżanowska, M. Wąsek-Wiaderek, *Prawo karne a Internet*..., s. 241 i n.; K.J. Jakubski, *Przestępczość komputerowa — zarys*..., s. 36 i n.

[49] Chodzi tutaj o możliwość wykorzystywania do ochrony danych osobowych konstrukcji wyrażonych w art. 23 i art. 24 k.c., służących do ochrony klasycznych dóbr osobistych. W piśmiennictwie podkreśla się, że ochrona danych osobowych postrzegana być winna jako wyspecjalizowana postać prawa do prywatności; zob. szerzej M. Safjan, *Ochrona danych*..., s. 10 i n. Por. też B. Gawlik, *Dobra osobiste. Zbiór orzeczeń Sądu Apelacyjnego w Krakowie*, Kraków–Zakamycze 1999, s. 282 i n.

[50] Szerzej na ten temat pisze S. Stanisławska-Kloc, *Przedmiot prawa autorskiego*..., s. 41–57 oraz J. Barta, R. Markiewicz, *Ochrona baz danych w systemie prawa autorskiego — stan obecny i perspektywy. Materiały konferencyjne „Infobazy" '97. Bazy danych dla nauki*, s. 20 i n.; J. Barta, R. Markiewicz, *Główne problemy*..., s. 54 i n.; A. Nowacka, *Prawnoautorska i patentowa ochrona programów komputerowych*, Warszawa 1995, s. 13 i n.

informacji, baz danych, programów komputerowych, twórczości komputerowej oraz innych dóbr wyrażanych przy pomocy zapisu cyfrowego, na które ataki dokonywane są przy wykorzystaniu nowoczesnych technik gromadzenia i przetwarzania informacji. Przyglądając się wprowadzanym do polskiego systemu prawnego rozwiązaniom, zauważyć można tendencję do zwiększania roli środków publicznoprawnych (administracyjnoprawnych) jako podstawy ochrony instytucjonalnej w sferze ochrony informacji, wyraźnie akcentującej jej aspekty prewencyjne.[51] Regulacje dotyczące ochrony różnorodnych dóbr prawnych, zawarte w wymienionych wyżej działach prawa, mają swe zakorzenienie w postanowieniach Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Rozwiązania prawne przyjęte w Konstytucji mają szczególne znaczenie dla prawnokarnych konstrukcji służących ochronie prawa do informacji oraz innych dóbr prawnych, zagrożonych atakami dokonywanymi przy wykorzystaniu nowoczesnych technologii cybernetycznych, wyznaczają bowiem konstytucyjny standard, w perspektywie którego rozstrzygane powinny być wszelkie konflikty, jakie towarzyszą ochronie poszczególnych wartości.[52]

III. OCHRONA INFORMACJI W POLSKIM SYSTEMIE PRAWA

6. Konstytucyjne fundamenty ochrony informacji zawarte zostały w kilku przepisach Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Na konstytucyjny standard prawa do prywatności oraz ochrony informacji składają się cztery grupy przepisów, a mianowicie przepisy: odnoszące się do ochrony prywatności, związane z ochroną informacji, dotyczące praw i wolności ekonomicznych, socjalnych i kulturalnych oraz określające konstytucyjne podstawy odpowiedzialności karnej. Wśród przepisów konstytucyjnych wyznaczających standard ochrony prywatności wymienić należy w pierwszej kolejności art. 47, który po raz pierwszy w dziejach polskiego konstytucjonalizmu określa jednoznaczną konstytucyjną podstawę ochrony prywatności. Zgodnie z jego brzmieniem: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci, dobrego imienia oraz do decydowania o swoim

[51] Zob. M. Safjan, *Ochrona danych*..., s. 13.

[52] Zob. M. Safjan, *Ochrona danych*..., s. 9 i n.; tenże, *Prawo do obrony życia prywatnego. Szkoła praw człowieka*, red. M.A. Nowicki, Warszawa 1996, s. 212 i n.; M. Wyrzykowski, *Ochrona danych osobowych — zagadnienia konstytucyjne* (w:) *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 23 i n.; W. Wróbel, *Uwagi wprowadzające*..., s. 969.

życiu osobistym".[53] Powołany przepis określa, jak stwierdza M. Safjan, „najbardziej pojemną i odnoszącą się do wszelkich dziedzin aktywności jednostki" ochronę sfery prywatności.[54] Wyrażona w nim norma konstytucyjna wprowadza zasadę zupełnej i bezwyjątkowej ochrony sfery prywatności jednostki, w tym także w zakresie informacji dotyczących samej jednostki, nie przewidując żadnych wyłączeń i ograniczeń w zakresie ochrony.[55] Swoistym dopełnieniem rozwiązania przyjętego w art. 47 Konstytucji jest treść przepisu jej art. 49, który gwarantuje wolność i ochronę komunikowania się. Konstytucja dopuszcza ograniczenia swobody komunikowania się jednostek, wprowadzając jednak warunek określenia tych ograniczeń w ustawie, uzupełniony o wymóg sprecyzowania przez ustawodawcę dopuszczalnych sposobów i form stosowania tych ograniczeń. Wśród przepisów odnoszących się do sfery ochrony informacji wskazać należy przepis art. 51 Konstytucji, który zawiera specjalną regulację dotyczącą zagadnienia ochrony danych osobowych. Zgodnie z jego brzmieniem: „1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów

[53] Podobne gwarancje zawierają przepisy art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych oraz art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności. Zob. szerzej: P. Hofmański, *Prawo do poszanowania prywatności (art. 17 Paktu i art. 8 Europejskiej Konwencji Praw Człowieka) a rozwiązania polskiego prawa karnego materialnego i procesowego* (w:) *Standardy praw człowieka a polskie prawo karne*, red. J. Skupiński i J. Jakubowska–Hara, Warszawa 1995, s. 253 i n.; tenże, *Konwencja europejska...*, s. 309–318; M.A. Nowicki, *Europejska Konwencja...*, s. 327–357; tenże, *Wokół Konwencji Europejskiej*, Warszawa 1992, s. 77–89. Co do cywilistycznej ochrony prywatności w prawie polskim w kontekście nowoczesnych technologii informacyjnych zob. szerzej E. Woch, *Sfera życia prywatnego i jej ochrona przed naruszeniami w Cyberprzestrzeni* (w:) *Internet 2000. Prawo–ekonomia–kultura*, red. R. Skubisz, Lublin 2000, s. 71–86.

[54] M. Safjan, *Ochrona danych...*, s. 15.

[55] Przepis art. 47 Konstytucji ma swoje odpowiedniki w aktach prawa międzynarodowego. Tak m.in. art. 12 Powszechnej Deklaracji Praw Człowieka stanowi: „Nikt nie będzie podlegać arbitralnemu wkraczaniu w jego życie prywatne, rodzinne lub korespondencję, ani też zamachom na jego honor lub reputację (...)"; art. 17 ust. 1 Międzynarodowego Paktu Praw Obywatelskich i Politycznych stanowi: „Nikt nie będzie poddany arbitralnej lub bezprawnej ingerencji w jego życie prywatne, rodzinne, mir domowy czy korespondencję, ani też zamachom na jego cześć i dobre imię"; wreszcie art. 8 ust. 1 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności stanowi: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji". Zob. szerzej w tej kwestii M.A. Nowicki, *Europejska Konwencja...*, s. 327–386; P. Hofmański, *Konwencja europejska ...*, s. 309–325; tenże, Wprowadzenie (w:) *Europejska Konwencji Praw Człowieka*, Kraków–Zakamycze 2000, s. 5–42.

danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa." Przytoczony przepis konstytucyjny zawiera kompleksową regulację odnoszącą się do sfery ochrony danych osobowych. Z punktu widzenia karnoprawnej problematyki ochrony informacji, na szczególne podkreślenie zasługuje wyrażone w ust. 1 powołanego wyżej przepisu konstytucyjnego prawo obywatela do nieujawniania informacji dotyczących jego osoby. Powyższy przepis zakreśla stosunkowo szerokie ramy konstytucyjnych gwarancji prawa do prywatności, od których odstępstwo określać mogą jedynie przepisy o randze ustawy. Na płaszczyźnie konstytucyjnej obowiązuje zasada swobodnego dysponowania przez daną osobę informacjami, które jej dotyczą. Ponadto przepis art. 51 Konstytucji określa podstawy i granice pozyskiwania, gromadzenia i udostępniania przez władze publiczne informacji o obywatelach, stanowiąc, iż gromadzeniu podlegać mogą tylko takie informacje dotyczące obywateli, które są niezbędne w demokratycznym państwie prawa. Zasada ograniczonego prawa do pozyskiwania, gromadzenia i udostępniania przez władze publiczne informacji o obywatelach koresponduje z wymienionym powyżej konstytucyjnym prawem do prywatności, stanowiąc jego negatywne normatywne dopełnienie.[56] Regulacja zawarta w art. 51 Konstytucji ustanawia prawo dostępu obywatela do urzędowych dokumentów i zbiorów danych, które zawierają informacje dotyczące danej osoby. Konstytucja ustanawia także prawo żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Wreszcie wskazać należy na treść artykułu 54 Konstytucji, który stanowi gwarancję wolności wyrażania poglądów oraz pozyskiwania i rozpowszechniania informacji. Wśród przepisów odnoszących się do sfery wolności i praw ekonomicznych, socjalnych i kulturalnych, jako istotny z punktu widzenia ochrony informacji wymienić wypada art. 76 Konstytucji, nakładający na władze publiczne obowiązek ochrony konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich prywatności oraz przed nieuczciwymi praktykami rynkowymi.[57] Wreszcie w rozważaniach poświęconych zagadnieniom odpowiedzialności karnej nie sposób pominąć art. 42 ust. 1 Konstytucji, określającego konstytucyjne standardy odpowie-

[56] Zob. szerzej M. Wyrzykowski, *Ochrona danych osobowych...*, s. 24–25.

[57] Zob. szerzej A. Bierć, *Ochrona danych...*, s. 113 i n.

działności karnej, oraz przepisu art. 2, wyrażającego zasadę demokratycznego państwa prawa.[58]

7. Rozwinięcie generalnych reguł dotyczących ochrony informacji, zamieszczonych w Konstytucji, zawierają przepisy ustaw zwykłych należących do różnych działów prawa. Regulacje odnoszące się do sfery ochrony informacji znajdują się w stosunkowo rozwiniętej formie w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,[59] w ustawie z dnia 28 września 1994 r. o rachunkowości,[60] w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[61] oraz w ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.[62] W każdej z nich zawarte są przepisy karne określające podstawy odpowiedzialności za zamachy skierowane przeciwko informacji.

Wymienione wyżej regulacje konstytucyjne pełnią w odniesieniu do zawartych w ustawach zwykłych szczególnych rozwiązań, które mają na celu ochronę informacji postrzeganej w kontekście nowoczesnych technologii cyfrowych, trzy istotne funkcje. Po pierwsze, wyznaczają fundamenty prawnej ochrony prywatności oraz ochrony informacji. Po drugie, wyznaczają nieprzekraczalne granice owej ochrony oraz wskazują przesłanki, jakie muszą zostać spełnione, aby dopuszczalna była ingerencja w sferę prywatności i ochrony informacji. Po trzecie wreszcie, określają standard konstytucyjny, jako podstawowy punkt odniesienia w przypadkach konfliktów między poszczególnymi chrniqnymi prawnie wartościami.[63]

[58] O znaczeniu zasady demokratycznego państwa prawa w płaszczyźnie odpowiedzialności karnej zob. szerzej A. Zoll, *Zasady prawa karnego w projekcie konstytucji*, Państwo i Prawo 1997, nr 3, s. 36 i n; tenże, *Nowa kodyfikacja karna...*, s. 45 i n.; M. Dąbrowska–Kardas, *O dwóch znaczeniach...*, s. 19 i n.; L. Kubicki, *Nowa kodyfikacja karna a Konstytucja RP*, Państwo i Prawo 1998, nr 9–10, s. 24–29.

[59] Dz.U. z 1994 r. Nr 24, poz. 83.

[60] Dz.U. z 1994 r. Nr 121, poz. 591.

[61] Dz.U. z 1997 r. Nr 133, poz. 883.

[62] Dz.U. z 1993 r. Nr 47, poz. 211.

[63] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 969–970.

IV. KARNOPRAWNA OCHRONA INFORMACJI ORAZ INNYCH DÓBR PRAWNYCH PRZED ZAMACHAMI DOKONYWANYMI PRZY WYKORZYSTANIU NOWOCZESNYCH TECHNOLOGII GROMADZENIA, PRZETWARZANIA I PRZESYŁANIA DANYCH

8. Każda z wymienionych wyżej ustaw szczególnych chroniących informacje zawiera przepisy karne, które mają na celu ochronę różnego rodzaju dóbr przed naruszeniami skierowanymi na zasoby informacyjne zgromadzone na nośnikach komputerowych oraz przed zamachami na inne niż informacja dobra dokonywanymi przy wykorzystaniu nowoczesnych technik gromadzenia i przetwarzania informacji. Niejako niezależnie od tej partykularnej kryminalizacji, karnoprawnej ochronie informacji służą przede wszystkim przepisy zawarte w nowym polskim Kodeksie karnym z 1997 r. Nawiązując do dyrektyw organizacji ponadnarodowych oraz wskazań Unii Europejskiej, w kilku rozdziałach zawiera on przepisy, które kryminalizują ataki na informację gromadzoną i przetwarzaną na komputerowych nośnikach oraz zamachy na inne dobra prawne dokonywane przy wykorzystaniu nowoczesnych technologii komputerowych. Zamieszczone w nowym Kodeksie karnym przepisy określające zasady odpowiedzialności za tzw. przestępstwa komputerowe funkcjonują w polskim ustawodawstwie obok przepisów karnych zawartych w pozakodeksowych ustawach szczególnych. Ta dwoistość regulacji powoduje, że w kilku co najmniej przypadkach zakresy zastosowania przepisów karnych zawartych w ustawach szczególnych i odpowiednich przepisów Kodeksu karnego krzyżują się, co sprawia, iż trudno jest jednoznacznie wskazać podstawę prawnokarnej ochrony konkretnego dobra prawnego oraz rozstrzygać zagadnienia kolizyjne. W powyższym kontekście dwie kwestie wymagają szczególnego zaakcentowania.

Pierwsza dotyczy przedmiotowego zakresu ochrony. Zarówno przepisy karne zawarte w wymienionych wyżej ustawach szczególnych, jak i przepisy Kodeksu karnego służą ochronie informacji gromadzonej, przetwarzanej i przesyłanej przez systemy komputerowe.[64] Co do zasady przepisy te chronią przy tym nie tyle samą informację oraz jej cyfrowe zapisy, ile raczej treść informacji wyrażającej określone wartości i dobra prawne, na które zamachy mogą być dokonywane przy wykorzystaniu nowoczesnych technologii informatycznych.

[64] O szczególnym powiązaniu informacji z innymi dobrami prawnymi, których odzwierciedleniem są określone zapisy informacyjne zgromadzone w cyfrowych urządzeniach gromadzących, przetwarzających i przesyłających informacje będzie mowa w dalszej części niniejszego opracowania.

Druga kwestia dotyczy immanentnego powiązania znamion określonych w tych przepisach typów czynu zabronionego z nowoczesnymi technikami gromadzenia i przetwarzania informacji w ten sposób, że albo charakterystyczne dla technologii cyfrowej zapisy informacji w postaci komputerowych baz danych lub programów komputerowych służących do obsługi systemów komputerowych stanowią przedmiot bezpośredniego oddziaływania danego przestępstwa rodzajowego, albo nowoczesna technologia cybernetyczna stanowi sposób lub narzędzie ataku na inne dobra prawne podlegające karnoprawnej ochronie.

Te dwa elementy, a więc charakterystyczny przedmiot ochrony karnoprawnej oraz specyficzny sposób lub narzędzie ataku, stanowiące podstawę kryminalizacji, stwarzają przesłanki do wyodrębnienia wzmiankowanej już wcześniej kategorii przestępstw, charakteryzujących się jednym lub oboma wymienionymi elementami, jako specyficznej grupy deliktów.

9. W odniesieniu do tych przestępstw, stanowiących podstawę kryminalizacji zachowań związanych z informacją zgromadzoną w nowoczesnych systemach komputerowych, od pewnego czasu w polskim piśmiennictwie karnistycznym oraz w siatce pojęciowej, którą posługują się praktycy stosowania prawa, coraz częściej wykorzystywane są terminy „przestępstwa komputerowe", „przestępczość komputerowa" czy „przestępstwa z wykorzystaniem komputera".[65] Analogiczne terminy występują w piśmiennictwie obcojęzycznym, w którym także poszukuje się kryteriów wyodrębnienia specjalnej kategorii deliktów powiązanych z nowoczesnymi technologiami gromadzenia, przetwarzania i przesyłania informacji.[66] Pojęcia te w zasadniczej większości

[65] Zob. szerzej A. Adamski, *Przestępstwa komputerowe*..., s. 15–24; tenże, *Prawo karne komputerowe*..., s. 30 i n.; R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, Warszawa 1993, s. 51 i n.;

[66] W piśmiennictwie niemieckim występują terminy *„Computerkriminalität"*, *„Computerstrafrecht"*, w literaturze angielskiej natomiast termin *„computer crime"*. Zob. w szczególności L. Bühler, *Ein Versuch*..., s. 448 i n.; K. Leicht, *Computerspionage*..., s. 45 i n.; T. Lenckner, M. Winkelbauer, *Computerkrominalität — Möglichkeiten und Grenzen des 2. WiKG (I)*, Computer und Recht 1986, s. 483 i n. K. Möhrenschlager, *Das neue Computerstraftecht*, Zeitschrift für Wirtschaft, Steuer, Strafrecht 1986, s. 128 i n.; tenże, *Neue gesetzliche Regelungen zur Computerkriminalität in den USA*, Zeitschrift für Wirtschaft, Steuer, Strafrecht 1985, s. 63 i n.; tenże, *Neue bundesstrafrechtliche Regelungen gegen die Fälschung und den Missbrauch von Kreditkarten u.a. in den USA, Zeitschrift für Wirtschaft, Steuer*, Strafrecht 1985, s. 216 i n.; tenże, *Das neue Computerstrafrecht*, Datenverarbeitung; Steuer, Wirtschaft, Recht. Zeitschrift für den Praxis des EDV (DSWR) 1986, s. 128 i n.; K. Tiedemann, *Computerkriminalität und Missbrauch von Bankomaten*, Wertpapier–Mitteilungen 1983, s. 1326 i n.; G. Stratenwerth, *Computerbetrug*, Schweizerische Zeitschrift für Strafrecht 1981, s. 229 i n.; P. Cramer (w:) Schönke/ Schröder, *Strafgesetzbuch. Kommentar*..., s. 1756 i n.; J.N. Gilbert, *Criminal Investigation*, New York–Toronto 1993, s. 419 i n.; P.A. Colier, B.J. Spaul, *Forensic sicence against computer crime in the United Kingdom*, Journal of the Forensic Science Society 1992, t. 32, nr 1, s. 27 i n.; D.B. Francis, *Computer Crime*, New York 1987, s. 14 i n.

przypadków używane są, jak podkreśla A. Adamski, w znaczeniu operacyjnym[67] — jako zbiorczy termin określający krąg patologicznych zjawisk związanych z powszechną w chwili obecnej komputeryzacją życia.[68] W literaturze polskiej brak jest do dzisiaj opracowania porządkującego kwestie terminologiczne w tym zakresie, które zawierałoby propozycje w miarę jednoznacznego zdefiniowania przytoczonych wyżej pojęć oraz wynikającego z przyjętej definicji zakreślenia kręgu desygnatów określonych terminów. Tym samym, zarówno w piśmiennictwie teoretycznym, jak i wśród praktyków stosowania prawa, terminom „przestępstwa komputerowe", „przestępczość komputerowa" oraz „przestępstwa popełniane z wykorzystaniem komputerów" przypisywane są różne treści, przy czym co do zasady przyjmowany *ad hoc* sposób definiowania i rozumienia określonego pojęcia wynika bezpośrednio z założonych przez autora celów i potrzeb badawczych oraz zadań, jakie spełniać ma dana publikacja lub z kontekstu, w jakim terminy te występują w praktyce.[69] Ów deficyt w sferze definiowania pojęć używanych dla opisu przestępczości powiązanej z wykorzystywaniem nowoczesnych technologii gromadzenia i przetwarzania informacji nie jest bynajmniej zjawiskiem wyłącznie polskim.[70] W piśmiennictwie krajów, które znacznie wcześniej niż Polska zetknęły się z problemem patologicznych zjawisk w sferze nowoczesnych technologii informatycznych również nie udało się wypracować jednoznacznej i precyzyjnej siatki terminologicznej.[71] Luki pojęciowej nie wypełniają także ustawodawcy, którzy wprowadzają cały szereg, nierzadko bardzo szczegółowych i detalicznych regulacji odnoszących się do sfery przestęp-

[67] A. Adamski, *Przestępstwa komputerowe*..., s. 15. Na nieokreśloność pojęcia „przestępstwa komputerowe" wskazują także inni autorzy. Zob. m.in. B. Fischer, *Przestępstwa komputerowe*..., s. 13–31; K.J. Jakubski, *Przestępczość komputerowa — zarys*..., s. 28 i n.

[68] Zob. B. Michalski, *Przestępstwa przeciwko mieniu. Rozdział XXXV Kodeksu karnego. Komentarz*, Warszawa 1999, s. 218–219.

[69] Podobnie zagadnienie kwestii terminologicznych w obszarze przestępczości związanej z automatycznym gromadzeniem, katalogowaniem, przetwarzaniem i przesyłaniem danych oraz informacji ujmuje A. Adamski, *Przestępstwa komputerowe*..., s. 15. Zdaniem K.J. Jakubskiego, pojęcie „przestępstwa komputerowe" oraz jego odpowiedniki traktowane być winny raczej jako hasła wywoławcze, nie zaś jako terminy określające zdefiniowane i określone zjawisko (*Przestępczość komputerowa*..., s. 34). Zob. też U. Sieber, *Przestępczość komputerowa i prawnokarna ochrona prawa do informacji*..., s. 223 i n.; R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, Warszawa 1993, s. 26 i n.; B. Fischer, *Przestępstwa komputerowe*..., s. 23 i n.; M. Trybus, *O tzw. przestępstwach komputerowych w kodeksie karnym z 1997 r.*, Rzeszowskie Zeszyty Naukowe 1999, nr 27, s. 54–71.

[70] Zob. U. Sieber, *Computerkriminalität und Strafrecht*, Berlin 1980, s. 27 i n.

[71] Zob. szerzej w tej kwestii U. Sieber, *Computerkriminalität*..., s. 27 i n.; tenże, *Informationstechnologie und Strafrechtsreform*..., s. 25 i n.; R. Sieg, *Strafrechtlicher Schutz gegen Computerkriminalität*, Juristische Ausbildung 1986, s. 352 i n. Por. też R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*..., s. 51 i n.; A. Adamski, *Przestępstwa komputerowe*..., s. 15–16.

czości związanej z nowoczesnymi technologiami informatycznymi, nie definiują jednak ustawowo takich pojęć, jak „przestępstwo komputerowe", „przestępstwo związane z wykorzystaniem komputera" czy wreszcie „przestępczość komputerowa".[72] Powody trudności związanych z jednoznacznym zdefiniowaniem analizowanych pojęć zdają się z jednej strony tkwić w zakorzenieniu analizowanych terminów w kilku dyscyplinach naukowych prawoznawstwa, z drugiej zaś — wynikać z charakteru przedmiotu regulacji, który jest trudny do precyzyjnego określenia oraz ulega permanentnym zmianom. Analizowane pojęcia przynależą do co najmniej trzech działów wyróżnianych w obrębie szeroko rozumianej karnistyki: prawa karnego materialnego, prawa karnego procesowego[73] oraz kryminologii;[74] wykorzystywane są także przez kryminalistykę.[75] Genetycznie pojęcia „przestępczość komputerowa" oraz „przestępstwa komputerowe" wywodzą się z kręgu kryminologii amerykańskiej, gdzie już w latach sześćdziesiątych zaczęto wykorzystywać te terminy jako zbiorczą nazwę dla określenia fenomenu przestępczości związanej integralnie z technologią cyfrową.[76] Pojęcie „przestępstwa komputerowe" zostało wprowadzone do literatury kryminologicznej dla opisu nowego zjawiska związanego z formami przestępnego działania, które nakierowane były na urządzenia zawierające zbiory danych zakodowanych i uporządkowanych cyfrowo. Przestępczość komputerowa stała się stosunkowo szybko modnym tematem badawczym kryminologii, w którym przedmiotem analizy uczyniono fenomen przestępczości popełnianej na styku z nowoczesnymi technologiami gromadzenia i przetwarzania informacji jako zjawiska społecznego. Szczegółowej analizie poddawano zwłaszcza kwestie rozmiarów tego ro-

[72] Badacz zagadnienia przestępczości komputerowej w Polsce, A. Adamski, stwierdza w tym kontekście, że „na stworzenie ogólnej definicji tych pojęć nie zdecydował się też żaden ze współczesnych ustawodawców" (*Przestępstwa komputerowe...*, s. 16).

[73] Zob. R. Kmiecik, *Prawnodowodowe aspekty...*, s. 7 i n.

[74] Zob. A. Adamski, *Przestępstwa komputerowe...*, s. 15.

[75] Zob. T. Tomaszewski, *Kryminalistyczna problematyka przestępczości komputerowej*, Problemy Kryminalistyki 1980, nr 143, s. 68 i n.; Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna*, Toruń 1996, s. 437–438; B. Hołyst, *Kryminalistyka*, Warszawa 1996, s. 242 i n.; K.J. Jakubski, *Przestępczość komputerowa...*, s. 265 i n.; B. Fischer, *Przestępstwa komputerowe...*, s. 13 i n.; R. Czachowski, P. Sienkiewicz, *Przestępcze oblicza komputerów...*, s. 52 i n.; W. Budzisz, *Badania kryminalistyczne na tle rozwoju przestępczości komputerowej w Polsce*, Problemy Kryminalistyki 1997, nr 214, s. 35–46.

[76] Opisując historię pojęcia „przestępstwa komputerowe" E.–J. Lampe stwierdza: *„Mit dem Begriff «Computer–Kriminalität» — er ist dem amerikanischen Begriff «computer–crime» nachgebildet — bezeichnet die heute in der kriminologischen Literatur vorherrschende Auffasung dasjenige Kriminelle (d.h. strafbare oder zumindest strafwürdige) Verhalten, dessen Mittel oder Zweck die Einwirkung oder pflichtwidrige Nichtwirkung auf die elektronische Datenverarbeitung (EDV) ist"* (*Die strafrechtliche Behandlung der sog. Computer–Kriminalität...*, s. 1). Zob. też G. Kaiser, *Kriminologie. Ein Lehrbuch*, 2. Auflage, Heidelberg 1995, s. 782 i n.

dzaju przestępczości, jej nasilenia, dynamiki oraz struktury.[77] Mimo iż to nauce kryminologii zawdzięczamy wprowadzenie do obiegu naukowego pojęcia „przestępstwa komputerowe", nie sposób zaprzeczyć, że terminy „przestępstwo komputerowe", „przestępstwo popełnione z wykorzystaniem komputera" czy „przestępczość komputerowa" są niejako naturalnie, immanentnie wręcz powiązane z prawem karnym materialnym. Pojęcia te przynależą do sfery prawa karnego materialnego, ponieważ właśnie ten dział prawa opisuje poszczególne przejawy zachowań jako przestępne. Zarazem pojęcia te mają swoją konotację karnoprocesową — wszak nowoczesne systemy automatycznego gromadzenia i przetwarzania danych bezpośrednio związane są z problematyką dowodową w procesie karnym,[78] zagadnieniem gwarancji procesowych, problematyką dozwolonych form i metod prowadzenia postępowania przygotowawczego, czynności operacyjnych itp. Wreszcie problematyka przestępstw komputerowych stanowi istotny fragment badań współczesnej kryminalistyki, poddającej je analizom w kontekście problemów związanych z rozpoznawaniem, wykrywaniem, dowodzeniem i zapobieganiem tego rodzaju przestępczości.[79] W każdym z tych działów prawa fenomen przestępczości komputerowej postrzegany jest w innej perspektywie, podlega porządkowaniu dla innych celów, wreszcie determinowany jest przez inne elementy różnicujące. Wszystko to sprawia, że występujące w literaturze definicje istotnie różnią się między sobą. Owe odmienności potęguje ogromna różnorodność postaci zjawiskowych przestępczości komputerowej, która sprawia, że wedle niektórych autorów nie sposób dzisiaj wyodrębnić „jednej — homogenicznej z punktu widzenia fenomenologii — przestępczości komputerowej".[80] W piśmiennictwie wyrażane są wręcz wątpliwości co do możliwości stworzenia prawniczej charakterystyki pojęcia „przestępstwa komputerowe", gdyż ter-

[77] Zob. szerzej C.K. Nicholson, R. Cunningham, *Computer crime*, American Criminal Law Review 1991, Nr 28, s. 393–406; D. Davies, *The nature of computer crime*, Computer and Law 1991, nr 2, s. 8–13; M. Wasik, *The Computer Misuse Act 1990*, Criminal Law Review 1990, s. 767–779; Co do zakresu badań kryminologicznych zob. szerzej J. Błachut, A. Gaberle, K. Krajewski, *Kryminologia*, Gdańsk 1999, s. 18–23.

[78] Zob. K.J. Jakubski, *Komputerowy nośnik informacji jako dokument w polskim procesie karnym*, Przegląd Policyjny 1997, nr 3 (47), s. 5–18; R. Kmiecik, *Prawnodowodowe aspekty...*, s. 7 i n.; J. Dzierżanowska, M. Wąsek–Wiaderek, *Prawo karne a Internet...*, s. 259–261. P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego*, t. I, *Komentarz*, Warszawa 1999, s. 855–867; K. Dudka, *Kontrola korespondencji i podsłuch w polskim procesie karnym*, Lublin 1998, s. 26 i n.; T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz*, Kraków–Zakamycze 1998, s. 472 i n.

[79] Por. T. Tomaszewski, *Kryminalistyczna...*, s. 68 i n.; Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna...*, s. 437–438; B. Hołyst, *Kryminalistyka...*, s. 242 i n.; B. Fischer, *Przestępstwa komputerowe...*, s. 32 i n.; K.J. Jakubski, *Przestępczość komputerowa — zarys...*, s. 35 i n.

[80] U. Sieber, *Przestępczość komputerowa...*, s. 39.

min ten wydaje się zarezerwowany wyłącznie dla badań kryminologicznych lub kryminalistycznych.[81] W radykalnym ujęciu wskazuje się, iż pojęcie „przestępstwa komputerowe" jest raczej hasłem, nie zaś nazwą, która określa istniejące realnie oraz dające się zdefiniować i opisać zjawisko normatywne,[82] cały zaś spór naukowy toczony wokół tej postaci przestępczości uznaje się za przejaw swoistej mody, w istocie sprowadzającej się do czynienia wiele hałasu o nic.[83]

Podkreślono już powyżej, że termin „przestępstwa komputerowe" stał się ostatnio niezwykle popularny także w Polsce, przebojowo wręcz wkraczając do literatury karnistycznej. Ostatnie lata obfitują w opracowania, które już w tytule zawierają określenie stanowiące połączenie rzeczownika „przestępstwo" oraz przymiotnika „komputerowe".[84] Widać w tym niewątpliwie z jednej strony próbę nadążania karnistów za wyzwaniami współczesności; wszak komputery, a zwłaszcza sieci komputerowe zawładnęły znaczną częścią życia społecznego. Z drugiej jednak strony, z uwagi na brak odpowiednich regulacji prawnych, rozważania poświęcone przestępczości komputerowej więcej mają wspólnego z analizą fenomenu przestępczości jako zjawiska, a także z analizą metody popełniania oraz wykrywania określonego rodzaju przestępczości niż z dogmatyką.

Wskazując na powiązania pojęcia „przestępstwa komputerowe" z czterema działami szeroko rozumianej karnistyki, zaznaczono zarazem, że w każdej z wymienionych dyscyplin problematykę przestępczości komputerowej

[81] Takie stanowisko prezentuje K.J. Jakubski, stwierdzając, że: „pojęcie przestępstwo komputerowe nie może stać się pojęciem prawnym. (...) Dlatego też przestępczość komputerową należy uważać za zjawisko kryminologiczne obejmujące wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, godzące bezpośrednio w przetwarzaną informację, jej nośniki i obieg w komputerze oraz całym systemie połączeń komputerowych, a także w sam sprzęt komputerowy oraz prawa do programu komputerowego" (*Przestępczość komputerowa...*, s. 282).

[82] Tak np. R. Sieg, *Strafrechtlicher Schutz gegen Computerkriminalität*, Jura 1986, s. 352 i n.

[83] Prezentujący takie stanowisko K.-M. Betzl jeden z pierwszych tekstów poświęconych przestępstwom komputerowym opatrzył charakterystycznym tytułem „Przestępczość komputerowa — wiele hałasu o nic?"(*Computerkriminalität — viel Lärum Nichts? Eine Richtig — Stellung*), DSWR 1971/72, nr 1, s. 475 i n.

[84] Zob. w szczególności: A. Adamski, *Prawne podstawy ścigania przestępstw komputerowych w Polsce*, Postępy Kryminalistyki 1997, nr 1, s. 44–56; tenże, *Karalność hackingu na podstawie przepisów kodeksu karnego z 1997 r.*, Przegląd Sądowy 1998, nr 11–12, s. 149–158; tenże, *Prawo karne komputerowe*, Warszawa 2000; K.J. Jakubski, *Przestępczość komputerowa: podział, definicja, możliwość jej ścigania i zapobiegania*, Postępy Kryminalistyki 1997, nr 1, s. 6–43; tenże, *Przestępczość komputerowa — podział i definicja*, Problemy Kryminalistyki 1997, nr 217, s. 31–38; M.T. Kolecki, *Przestępstwa komputerowe w USA w ujęciu prawa stanowego*, Palestra 1992, nr 5–6, s. 52–63; P. Sikora, *Przestępstwa komputerowe w ujęciu nowego kodeksu karnego*, Acta Uniwersitatis Wratislaviensis, Prawo CCLXVI, Wrocław 1999, s. 347–355.

analizuje się pod innym kątem, wykorzystując inne metody badawcze, oraz zmierza się do odmiennych celów. Stąd też uniformizacja siatki terminologicznej, jej pełne ujednolicenie, stanowi na razie jedynie idealizacyjny postulat. W kontekście powyższej niejednorodności podejścia do zagadnienia przestępczości komputerowej oraz daleko idącej nieprecyzyjności pojęć wykorzystywanych dla opisu badanego zjawiska, która stanowi jej konsekwencję, konieczne jest dokonanie na wstępie zabiegu porządkującego. Sposób patrzenia na przestępczość komputerową, a w konsekwencji — metoda definiowania podstawowych pojęć w tym zakresie, uzależnione są w znacznej mierze od tego, na obszarze jakiej dyscypliny naukowej kwestia ta poddawana ma być analizie. W niniejszym opracowaniu podstawowym punktem odniesienia będą odpowiednie przepisy obowiązujących aktów prawnych, określające odmiany przestępstw powiązanych z nowoczesnymi technologiami cyfrowymi, treść zaś wywodu stanowić bedzie ich dogmatyczna analiza. Takie zakreślenie pola badawczego wyraźnie wskazuje na pierwszeństwo tych ujęć terminologicznych, które wypracowane zostały w piśmiennictwie poświęconym zagadnieniom prawa karnego materialnego. Ujęcia karnoprocesowe, kryminalistyczne oraz kryminologiczne stanowić będą w powyższym kontekście co najwyżej podstawę pewnych dopełnień.

Przyjęcie za podstawowy punkt odniesienia sposobów rozumienia pojęcia „przestępstwa komputerowe" w prawie karnym materialnym, ograniczając nieco zakres możliwych rozbieżności terminologicznych poprzez usunięcie z pola badań kwestii karnoprocesowych, kryminalistycznych i kryminologicznych, bynajmniej nie oznacza automatycznego rozwiązania wszelkich zagadnień kwestii spornych. W samym obszarze prawa karnego materialnego istnieje bowiem kilka alternatywnych sposobów rozumienia pojęcia „przestępstwa komputerowe". Poszczególne koncepcje terminologiczne, prowadzące do wyznaczenia zakresu zjawiska określanego jako „przestępstwa komputerowe", związane są nierozerwalnie ze stadiami rozwoju tej sfery karnistyki.

Fenomen przestępczości komputerowej swymi korzeniami sięga naruszeń zbiorów danych osobowych, gromadzonych na nowoczesnych nośnikach informacji. Już we wczesnych latach sześćdziesiątych w związku z pojawieniem się na szeroką skalę komputerowych zbiorów danych osobowych zaczęto obserwować nasilające się zjawisko naruszania prawa do informacji oraz prywatności przy wykorzystaniu nowoczesnych technik komputerowych. Wprowadzone do ustawodawstwa specjalne typy przestępstw, stanowiące podstawę kryminalizacji tego rodzaju ataków na dane osobowe (chronione zasoby informacji), zaczęto wówczas określać mianem przestępczości komputerowej. Przestępstwa te określa się w piśmiennictwie jako tzw. klasyczne

przestępstwa komputerowe.[85] Pierwotnie pojęcie „przestępstwa komputerowe" służyło więc do oznaczania przestępstw skierowanych przeciwko danym osobowym zgromadzonym na specyficznych, komputerowych nośnikach informacji.[86] W niewiele lat później, bo już w połowie lat siedemdziesiątych tak wąsko rozumianą grupę przestępstw komputerowych zaczęto w piśmiennictwie karnistycznym gwałtownie rozszerzać. Powodem owej ekspansji pojęcia „przestępstwa komputerowe" na zachowania niestanowiące naruszeń prawa do informacji i danych osobowych był fakt rozpowszechnienia techniki komputerowej w sferze obrotu gospodarczego, a w konsekwencji powstania nowej kategorii zamachów na klasyczne dobra prawne chronione przez tzw. przestępstwa gospodarcze, dokonywanych za pomocą nowoczesnej techniki komputerowej.[87] W tej grupie przestępstw umieszczano z reguły zamachy przyjmujące postać różnego rodzaju manipulacji komputerowych, sabotażu, szantażu, hackingu komputerowego, szpiegostwa oraz kradzieże programów komputerowych, a z biegiem czasu także i inne formy piractwa towarowego.[88] W ostatnim okresie pojęcie „przestępstwa komputerowe" wykorzystywane jest coraz częściej dla zbiorczego określenia nie tylko dwóch wymienionych wyżej kategorii przestępstw, lecz także jako nazwa nadrzędna dla przestępstw stanowiących zamachy na wszelkie tradycyjne dobra prawne, dokonywane przy pomocy nowoczesnej techniki komputerowej.[89] Zastanawiająca jest skala rozpiętości pojęcia „przestępstwa komputerowe", które obecnie obejmuje zarówno ataki na zbiory informacji zgromadzone na odpowiednich nośnikach, ataki na tradycyjne dobra prawne w sferze obrotu gospodarczego dokonywanych przy pomocy nowoczesnych technologii komputerowych oraz ataki na dobra prawne najbardziej już typowe dla prawa karnego, takie jak wolność lub cześć, dokonywane przy wykorzystaniu nowoczesnych technologii komputerowych.[90] Podkreślić wypada, że rozszerzaniu zakresu pojęcia „przestępstwa komputerowe" towarzyszy rozmywanie się lub wręcz zanik ustawowych cech stanowiących o specyfice tego rodzaju deliktów.

[85] Zob. A. Adamski, *Karalność hackingu...*, s. 149.

[86] Zob. szerzej U. Sieber, *Przestępczość komputerowa...*, s. 224; tenże, *Computerkriminalität...*, s. 39 i n.

[87] U. Sieber podkreśla, że delikty gospodarcze popełniane przy wykorzystaniu komputerów, uchodzą dzisiaj za rdzeń tzw. przestępczości komputerowej. Zob. szerzej U. Sieber, *Przestępczość komputerowa...*, s. 225.

[88] Por. U. Sieber, *Przestępczość komputerowa...*, s. 225.

[89] Tak m.in. B. Fischer określa przestępstwa komputerowe jako „czyny skierowane zarówno przeciwko systemowi komputerowemu (komputer–cel), jak i popełniane przy jego użyciu (komputer–narzędzie)" (*Przestępstwa komputerowe...*, s. 24). Zob. też podobne ujęcie K.J. Jakubski, *Przestępczość komputerowa — zarys problematyki...*, s. 34.

[90] Zob. U. Sieber, *Przestępczość komputerowa...*, s. 225.

W kontekście przedstawionych wyżej uwag terminologicznych można stwierdzić, iż obecnie grupa przestępstw komputerowych jest niezwykle różnorodna, a pojęciem „przestępstwa komputerowe" w obszarze prawa karnego materialnego obejmuje się różnorodne odmiany deliktów, dające się pogrupować w trzy zasadnicze kategorie.

Pierwsza obejmuje zamachy skierowane na specyficzne dobro prawne, jakim jest informacja, powiązana immanentnie z nowoczesnymi technologiami gromadzenia, przetwarzania i przesyłania informacji. W tej grupie podstawowym przedmiotem ochrony jest właśnie informacja, natomiast przedmiot oddziaływania, na który skierowane są czynności sprawcy stanowią: komputer, systemy komputerowe, komputerowe bazy danych, procesy cyfrowego gromadzenia, przetwarzania i przesyłania informacji. W pewnych sytuacjach komputer lub elementy konieczne do jego prawidłowego funkcjonowania albo komputerowe bazy danych stanowią podlegające ochronie dobro prawne i zazem przedmiot zamachu. Ta część przestępstw komputerowych stypizowana została w rozdziale XXXIII Kodeksu karnego z 1997 r. pt. „Przestępstwa przeciwko ochronie informacji". Rozdział ten grupuje w szczególności: hacking komputerowy (art. 267 § 1 k.k.); nielegalny podsłuch i inwigilację przy użyciu urządzeń technicznych (art. 267 § 2 k.k.); naruszenie integralności zapisu informacji (art. 268 § 2 k.k.); sabotaż komputerowy (art. 269 § 1 i 2 k.k.).[91] Ponadto część przestępstw o charakterze zbliżonym do typów zgromadzonych w rozdziale XXXIII k.k. zawarta jest w rozdziale XXXV k.k. z 1997 r. pt. „Przestępstwa przeciwko mieniu". Typy określone w tym rozdziale nie chronią, co prawda, informacji jako podstawowego dobra prawnego, lecz określają przedmiot ochrony w taki sposób, iż obejmuje on elementy konieczne dla prawidłowego funkcjonowania komputerów. Do tych przestępstw zaliczyć należy: nielegalne uzyskanie programu komputerowego (art. 278 § 2 k.k.) oraz paserstwo komputerowe (art. 293 § 1 w zw. z art. 291 k.k. lub w zw. z art. 292 k.k.). Tę kategorię przestępstw określa się w piśmiennictwie czasami jako „przestępstwa *stricte* komputerowe".[92]

Druga kategoria obejmuje delikty, w których przedmiotem zamachu nie jest informacja podlegająca cyfrowemu przetworzeniu poprzez system komputerowy, lecz tradycyjne dobra prawne chronione przez przepisy prawa karnego, których naruszenie dokonuje się przy wykorzystaniu nowoczesnych tech-

[91] Rozdział grupujący podobną kategorię przestępstw znajduje się także m.in. w nowym rosyjskim kodeksie karnym z 1996 r., nosząc tytuł „Przestępstwa w dziedzinie informacji komputerowej"; zob. szerzej A. Adamski, *Przestępstwa komputerowe...*, s. 17 i n.

[92] Tą konwencją terminologiczną posługuje się w polskiej literaturze przede wszystkim A. Adamski (*Przestępstwa komputerowe...*, s. 17).

nik gromadzenia i przetwarzania informacji. Komputer stanowi zatem w odniesieniu do tej kategorii przestępstw narzędzie popełnienia czynu zabronionego; przy czym komputer, a nieco szerzej — elektroniczne technologie gromadzenia i przetwarzania danych — stanowią w tej grupie narzędzie popełnienia przestępstwa, precyzyjnie określone w ustawowym opisie danego rodzaju przestępstwa rodzajowego.[93] Do tej kategorii przestępstw zaliczyć można przestępstwo oszustwa komputerowego (art. 287 k.k.); oszustwo telekomunikacyjne (art. 285 k.k.); szpiegostwo komputerowe (art. 130 § 3 k.k.). Z uwagi na przyjętą w art. 115 § 14 k.k. definicję dokumentu,[94] do tej grupy zaliczyć można także przestępstwo zniszczenia lub pozbawienia mocy dowodowej dokumentu elektronicznego (art. 276 k.k.); fałszerstwo komputerowego zapisu informacji stanowiącego dokument (art. 270 § 1 k.k.); nierzetelne prowadzenie dokumentacji działalności gospodarczej (art. 303 k.k.); fałszerstwo kart płatniczych (art. 310 k.k.).[95]

Wreszcie trzecia kategoria obejmuje delikty stanowiące zamachy na tradycyjne dobra prawne dokonywane przy pomocy nowoczesnych urządzeń, które służą do cyfrowego gromadzenia i przetwarzania danych, z tym jednak, że sposób popełnienia przestępstwa przy wykorzystaniu tych technologii nie znajduje odzwierciedlenia w ustawowym opisie danej odmiany przestępstwa rodzajowego.[96] Do tej grupy przestępstw zaliczyć można m.in. rozpowszechnianie treści pornograficznych poprzez sieć Internet (art. 202 k.k.); zniesławienie (art. 212 k.k.); zniewagę (art. 216 k.k.); groźbę karalną (art. 190 k.k.).[97]

[93] Por. A. Adamski, *Prawo karne komputerowe...*, s. 31.

[94] Definicja dokumentu obejmuje także „zapis na komputerowym nośniku informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne". Zob. szerzej w tej kwestii A. Wąsek (w:) M. Kalitowski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny. Komentarz*, t. II, Gdańsk 1999, s. 406–409.

[95] A. Adamski wymienione wyżej w grupie trzeciej przestępstwa zalicza do kręgu przestępstw komputerowych, przydając im zbiorczą nazwę „przestępstwa komputerowe przeciwko wiarygodności dokumentów, obrotowi gospodarczemu i pieniężnemu" (*Przestępstwa komputerowe...*, s. 90–107). Zob. też J. Dzierżanowska, M. Wąsek–Wiaderek, *Prawo karne a Internet...*, s. 253 i n.

[96] Tak szerokie ujęcie przestępstw komputerowych prezentowane jest w opracowaniach z zakresu kryminalistyki. Tak np. wedle T. Tomaszewskiego, przestępstwem komputerowym jest „każdy czyn przestępny, w którym komputer jest albo narzędziem, albo przedmiotem przestępstwa" — Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna...*, s. 437–438. Dla R. Czechowskiego i P. Sienkiewicza przestępstwa komputerowe to „wszelkie bezprawne, nieetyczne i nie upoważnione zachowanie odnoszące się do procesu przetwarzania i (lub) przekazywania danych" (*Przestępne oblicza komputerów...*, s. 52). Wreszcie, wedle B. Hołysta, przestępstwo komputerowe to każdy akt przynoszący stratę, szkodę lub uszkodzenia, do których dokonania wykorzystano systemy przetwarzania danych (*Kryminalistyka...*, s. 242).

[97] A. Adamski, *Przestępstwa komputerowe...*, s. 18 i n.; J. Dzierżanowska, M. Wąsek–Wiaderek, *Prawo karne a Internet...*, s. 248 i n.

Poszukując cech charakteryzujących kategorię przestępstw komputerowych podnieść należy, iż samo wskazanie na nowoczesne techniki komputerowe jako środek lub narzędzie popełnienia przestępstwa sprawia, że ten element — stanowiący charakterystyczną cechę przestępstwa komputerowego — daleki jest od jednoznaczności. Jak podkreśla A. Adamski, elektroniczne sposoby przetwarzania danych mogą być wykorzystywane jako narzędzie popełniania bardzo wielu przestępstw, w tym także takich, których opis zachowania przestępnego nie wyszczególnia postaci czynności sprawczej polegającej na wykorzystaniu nowoczesnych technik gromadzenia i przetwarzania informacji.[98] Z punktu widzenia specyficznej kategorii deliktów, jaką tworzą przestępstwa komputerowe, sama możliwość wypełnienia znamion danego typu czynu zabronionego przy wykorzystaniu nowoczesnej techniki komputerowej nie wydaje się więc przesłanką wystarczającą dla uzasadnienia zaliczenia tego rodzaju przestępstw do kategorii przestępstw komputerowych.[99] Jeśli w ogóle sensowne jest posługiwanie się pojęciem „przestępstwa komputerowe", określającym taką kategorię przestępstw, która charakteryzuje się specyficznymi właściwościami, odróżniającymi je od innych rodzajów przestępstw, to wyznacznika tej szczególnej odmiany przestępstw poszukiwać należy w ich ustawowej charakterystyce, nie zaś na obszarze faktycznych środków i sposobów popełnienia czynu zabronionego, możliwych z uwagi na rozwój nowoczesnych technologii.[100] Uznając ustawową charakterystykę za podstawowy element przesądzający o możliwości zaliczenia danego deliktu do kategorii przestępstw komputerowych, przypomnieć wypada, że ten rodzaj przestępczości genetycznie wywodzi się z kręgu takich typów, w których przedmiotem ochrony były: odpowiedni rodzaj informacji zgromadzonej w systemie komputerowym, komputerowe bazy danych, programy komputerowe lub utwory komputerowe. Innymi słowy, w punkcie wyjścia ustawowa charakterystyka przedmiotu ochrony pozwalała zaliczyć dane prze-

[98] Autor ten trafnie wskazuje, że „używając poczty elektronicznej można dopuścić się zniesławienia (art. 212), zniewagi (art. 216) lub groźby karalnej (art. 190), przesyłając na adres innej osoby wiadomość o treści wypełniającej znamiona tych przestępstw". Ponadto A. Adamski wskazuje kilka innych typów przestępstw, które mogą być popełnione przy wykorzystaniu nowoczesnych technik komputerowych — zob. szerzej A. Adamski, *Przestępstwa komputerowe...*, s. 18.; tenże, *Prawo karne komputerowe...*, s. 31 i n.

[99] Nie oznacza to, iż na przykład w badaniach kryminologicznych lub kryminalistycznych taka kategoria przestępstw nie może być zaliczana do kręgu przestępstw komputerowych.

[100] Podobne stanowisko zajmuje w tej kwestii A. Adamski, stwierdzając, że „wspólną cechą tych czynów jest bowiem odwoływanie się ich znamion ustawowych do elementów szeroko pojętej techniki komputerowej. Można więc stwierdzić, że są one przestępstwami komputerowymi nie ze względu na przedmiot zamachu, lecz ustawowo określony sposób działania sprawcy" (*Prawo karne komputerowe...*, s. 32).

stępstwo do kategorii przestępstw komputerowych.[101] Jeśli zatem obecnie, uznając tak zakreślony krąg przestępstw komputerowych za zbyt wąski, dokonuje się rozszerzenia kategorii przestępstw komputerowych, to konieczne jest poszukiwanie kryteriów charakteryzujących tę grupę na płaszczyźnie ustawowego opisu znamion. W konsekwencji pojęciem „przestępstwa komputerowe" objąć można także te delikty, w których przedmiot ochrony nie ma bynajmniej charakteru *stricte* komputerowego, jednak w ustawowym opisie znamion sposób działania sprawcy lub wykorzystywane przez niego narzędzia, które prowadzą do realizacji znamion, zostały przez ustawodawcę określone jako wykorzystywanie nowoczesnej techniki komputerowej. Innymi słowy, sposób wypełnienia znamion typu polegający na wykorzystaniu przez sprawcę techniki komputerowej decydować może o zaliczeniu danego przestępstwa do kategorii komputerowych jedynie wówczas, gdy ustawowy opis znamion danego typu wyraźnie wskazuje, iż musi lub może być on popełniony przy użyciu komputera, mimo że dane przestępstwo skierowane jest przeciwko innemu niż informacja dobru prawnemu. Przyjmując taki sposób charakterystyki pojęcia „przestępstwa komputerowe" na obszarze prawa karnego materialnego, do tej grupy przestępstw zaliczyć należy następujące typy czynu zabronionego stypizowane w Kodeksie karnym z 1997 r.: hacking komputerowy (art. 267 § 1 k.k.); nielegalny podsłuch i inwigilację przy użyciu urządzeń technicznych (art. 267 § 2 k.k.); naruszenie integralności zapisu informacji (art. 268 § 2 k.k.); sabotaż komputerowy (art. 269 § 1 i 2 k.k.); nielegalne uzyskanie programu komputerowego (art. 278 § 2 k.k.); paserstwo programu komputerowego (art. 293 § 1 w zw. z art. 291 lub w zw. z art. 292 k.k.); oszustwo komputerowe (art. 287 k.k.); oszustwo telekomunikacyjne (art. 285 k.k.); szpiegostwo komputerowe (art. 130 § 2 k.k.); przestępstwo zniszczenia lub pozbawienie mocy dowodowej dokumentu elektronicznego (art. 276 k.k.); fałszerstwo komputerowego zapisu informacji stanowiącego dokument (art. 270 § 1 k.k.); nierzetelne prowadzenie dokumentacji działalności gospodarczej (art. 303 k.k.); fałszerstwo kart płatniczych (art. 310 k.k.).[102]

W kontekście przedstawionych wyżej uwag można stwierdzić, że pojęciem „przestępstwa komputerowe" określać będziemy w dalszej części niniejszego opracowania tylko dwie z wymienionych wyżej kategorii przestępstw: po pierwsze, te, w których przedmiot zamachu ma charakter komputerowy, a więc jest nim konkretnie system komputerowy, program komputerowy, utwór komputerowy lub komputerowa baza danych; po drugie, przestępstwa, które mają inny niż „komputerowy" przedmiot ochrony, jednak w ustawowym opisie typu ustawodawca wyraźnie wskazuje, że realizacja znamion może lub musi być dokonana przy pomocy nowoczesnych technik gromadzenia i przetwarzania danych.[103]

Wszelkie pozostałe kategorie przestępstw, w tym zwłaszcza przestępstwa, które mogą być popełniane przy użyciu nowoczesnych technologii przetwarzania informacji, jednak nie mają tego elementu wyraźnie zaznaczonego w ustawowym opisie znamion — nie stanowią przestępstw komputerowych.[104] Dla określenia tej kategorii deliktów w obszarze prawa karnego materialnego można wykorzystywać zaproponowaną przez A. Adamskiego nazwę „przestępstwa popełniane przy wykorzystaniu komputera", podkreślając zarazem kryminologiczny charakter kryterium, które stanowią podstawę wyodrębnienia tej klasy zachowań.[105]

Przedstawione wyżej rozróżnienie terminologiczne nie opiera się na jakichś stałych normatywnych właściwościach przestępstw zaliczanych do jednej z wymienionych kategorii. Tym też różni się ono od podziałów przestępstw występujących w dogmatyce prawa karnego. Obie nazwy mają raczej konwencjonalny charakter, pełniąc przede wszystkim funkcję klasyfikującą materiał normatywny.[106] Wyróżnienie kategorii przestępstw komputerowych niewątpliwie stanowi znak czasów, w których prawie wszystkie przejawy egzystencji człowieka powiązane są z cybernetycznie gromadzoną, przetwarzaną i przesyłaną informacją. Zarazem jednak wyodrębnienie kategorii przestępstw kom-

[101] Zob. J. Lampe, *Die strafrechtliche Behandlung der sog. Computer–Kriminalität*, Goltdammer's Archiv für Strafrecht 1975, s. 1 i n.; T. Lenckner, *Computerkriminalität und Vermögensdelikte*, Berlin 1981, s. 23 i n.; J. Baumann, *Strafrecht und Witrschaftskriminalität*, Juristenzeitung 1983, s. 935 i n.

[102] Zakreślony w niniejszym opracowaniu krąg tzw. przestępstw komputerowych jest nieco węższy od katalogu przestępstw uznawanych za komputerowe prezentowanych w innych opracowaniach. Por. w szczególności A. Adamski, *Przestępstwa komputerowe...*, s. 17 i n.; B. Fischer, *Przestępstwa komputerowe...*, s. 23–102.

[103] Przyjęta powyżej definicja przestępstw komputerowych została wykorzystana dla klasyfikacji przestępstw stypizowanych w Kodeksie karnym z 1997 r. Jest oczywiste, iż typy przestępstw określone w ustawach szczególnych, spełniające konstytutywne dla przyjętej definicji kryteria, także zaliczane będą do grona przestępstw komputerowych. Do tej grupy zaliczyć można w szczególności przestępstwa określone w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych — zob. szerzej M. Mozgawa, J. Radoniewicz, *Przepisy karne w prawie autorskim. Zagadnienia teorii i praktyki*, Prokuratura i Prawo 1997, nr 7–8, s. 7 i n.; R. Kmiecik, *Prawnodowodowe aspekty...*, s. 7 i n.; R. Zakrzewski, *Prawne instrumenty zwalczania piractwa komputerowego*, Kontrola Państwowa 1995, nr 1, s. 99–110.

[104] Stąd też trudno zaaprobować w obszarze prawa karnego definicję przestępstw komputerowych zaproponowaną przez B. Fischera, dla którego przestępstwa komputerowe to wszelkie czyny „skierowane przeciwko systemowi komputerowemu (komputer–cel), jak i popełniane przy jego użyciu (komputer–narzędzie)", co nie oznacza oczywiście, iż tego rodzaju ujęcie nie może być z powodzeniem wykorzystywane na przykład w kryminalistyce.

[105] Zob. A. Adamski, *Przestępstwa komputerowe...*, s. 20.

[106] Analogicznie kwestię tę postrzega A. Adamski, *Prawo karne komputerowe...*, s. 32.

puterowych jako specyficznej grupy deliktów jest niezwykle silnie uwikłane w doczesność, co sprawia, iż pojawienie się zmian w technologii cyfrowej spowodować może zmianę terminologii stosowanej do tej grupy przestępstw.[107] Stąd też, poddając dogmatycznej analizie tzw. przestępstwa komputerowe warto pamiętać, iż poprzez odwołanie się do aktualnie dominującego w technologii cyfrowej paradygmatu łączymy ze sobą przestępstwa różniące się niekiedy istotnie jurydyczną charakterystyką. Poszukując najbardziej adekwatnej nazwy dla przestępstw związanych z nowoczesnymi technologiami, coraz częściej w piśmiennictwie wykorzystuje się nazwę „przestępstwa związane z technologią przetwarzania informacji" lub „przestępstwa związane z procesem komunikowania się".[108] Oba określenia wskazują na charakteryzujący omawianą grupę przestępstw element w postaci informacji, która jest nośnikiem treści relewantnych prawnie oraz podlega procesowi przekazu. Odmienność przestępstw związanych z wykorzystaniem nowoczesnych technologii cyfrowych w stosunku do pozostałych przestępstw wynika z faktu, iż atak na dobro prawne dokonuje się poprzez zamach na informację będącą odzwierciedleniem tego dobra lub poprzez zamach na proces przetwarzania bądź przekazywania tej informacji. Stąd też w pewnym sensie wszystkie przestępstwa zaliczane do grupy „komputerowych" są przestępstwami informacyjnymi, albowiem ich popełnienie dokonuje się zawsze poprzez określone oddziaływanie na informację.

10. Podejmując próbę dokonania analizy aktualnego stanu prawnego w sferze tzw. przestępstw komputerowych oraz poszukując szczególnych podstaw ochrony informacji w nowoczesnym społeczeństwie informatycznym, nie sposób pominąć kilku uwag odnoszących się do rodzajowego przedmiotu ochrony. Wykorzystywana w prawoznawstwie siatka pojęciowa w zakresie prawnej reglamentacji działań, których przedmiotem jest informacja, uległa w ostatnim ćwierćwieczu istotnym przeobrażeniom. Samo pojęcie informacji, jako przedmiotu ochrony, nabrało pod wpływem wykorzystywania

[107] Tendencje zmiany nazewnictwa tej kategorii przestępstw pojawiły się już w drugiej połowie lat dziewięćdziesiątych w literaturze amerykańskiej oraz niemieckiej. W piśmiennictwie anglojęzycznym coraz częściej wykorzystuje się pojęcia „cyberprzestępstwa", „przestępstwa związane z technologią cyfrową", „przestępstwa internetowe" czy „przestępstwa związane z technologią przetwarzania informacji". Zob. szerzej A. Adamski, *Prawo karne komputerowe...*, s. 33. W piśmiennictwie niemieckim zastępuję się pojęcie „przestępstwa komputerowe" terminami „przestępstwa informacyjne" (*„Informationsstrafrecht"*) lub „przestępstwa związane z procesem komunikowania się" (*„Kommunikationskriminalität"*); zob. szerzej W. Müller, *Aktuelle Probleme...*, s. 19; K. Tiedemann (w:) *Leipziger Kommentar. Gross Kommentar, § 263 a StGB*, RN 1, s. 17.

[108] *„Kommunikationskriminalität"* (W. Müller, *Aktuelle Probleme...*, s. 19).

nowoczesnych, cybernetycznych technologii nowego znaczenia, zasadniczo odbiegającego od tradycyjnego rozumienia tego terminu. Jeszcze kilkadziesiąt lat temu informację rozumiano czasownikowo, jako specyficzną czynność związaną z procesem komunikowania się. Takie rozumienie informacji pozostawało w zgodzie z pierwotnym, słownikowym znaczeniem tego pojęcia, jako synonimu czynności polegających na przekazywaniu określonych wiadomości.[109] Obecnie, w kontekście powszechnego wykorzystywania cybernetycznych technologii gromadzenia i przetwarzania danych, w piśmiennictwie prawniczym, w tym także w literaturze karnistycznej pojawiają się tendencje do odmiennego rozumienia pojęcia „informacja", zmierzającego jednoznacznie w kierunku substancjalnego odczytywania treści tego terminu. W niektórych pracach przyjmuje się, że informacja oznacza obecnie nie tyle pewien proces komunikowania się (informowania), ile raczej samą wiadomość, określony znak kulturowy kryjący pewną sensowną treść.[110] Informacja w tym ujęciu uzyskuje jednoznacznie materialny (substancjalny) charakter; zlewa się ze znakiem (danymi) służącym do jej wyrażenia. Termin „informacja" nabiera zatem podwójnego znaczenia, określa bowiem zarówno odpowiedni znak kulturowy kryjący pewną sensowną treść, jak i wynik odczytania tego znaku, a więc ową treść właśnie.[111] W ujęciu alternatywnym, prezentowanym przez inną część piśmiennictwa specjalistycznego, także odchodzi się od tradycyjnego, słownikowego rozumienia pojęcia „informacja". Zarazem jednak, w przeciwieństwie do koncepcji utożsamiającej pojęcie informacji i znaku (danych), koncepcja ta nie przydaje desygnatom tego terminu materialnego substratu, lecz poszukuje dystynkcji między pojęciem „informacja" a terminem „dane".[112] W opracowaniach mieszczących się w ramach tego nurtu wskazuje się, że informacja ze swej natury „nie ma charakteru materialnego i nie jest rzeczą, lecz procesem zachodzącym pomiędzy umysłem człowieka i działającym na niego bodźcem".[113] Określenie informacji w tym ujęciu w pewnym sensie

[109] W ujęciu słownikowym „informacja" to „powiadomienie o czymś, zakomunikowanie czegoś, wiadomość, wskazówka, pouczenie" (*Słownik języka polskiego*, t. 1, red. M. Szymczak, Warszawa 1996, s. 739). Informacja definiowana jest więc co do zasady czasownikowo.

[110] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 968.

[111] *Ibidem*.

[112] Tak np. J. Welp: *„Unterteilt den hieran angelehnten Datenbegriff für den strafrechtlichen Gebrauch in zwei Ebenen, eine erste der Semantik und eine zweite der Syntax, die Bedeutung (Inhalt) eines Datums von seiner Darstellung (Zeichen) abschichten" — Dantenveränderung (§ 303 a StGB)*, Teil I, IuR 1988, s. 443–445. Podobnie Th. Gerhards, *Computerkriminalität...*, s. 27 i n.; T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, § 202a, s. 1350. W polskiej literaturze karnistycznej stanowisko takie prezentuje m.in. A. Adamski, *Przestępstwa komputerowe...*, s. 26–29.

[113] A. Adamski, *Przestępstwa komputerowe...*, s. 26–27.

nawiązuje więc do tradycyjnego, słownikowego rozumienia tego terminu jako specyficznego procesu przekazywania wiadomości.[114] Z drugiej strony informacji przeciwstawia się pojęcie „dane", traktowane jako „zapis określonej informacji lub jej reprezentację", który może przybierać różną formę (literową, cyfrową, dźwiękową, rysunkową).[115] W tym ujęciu dane, będąc zapisem informacji, są więc specyficznym medium, za pomocą którego informacja może być przekazywana.[116] W świetle przedstawianej konwencji terminologicznej w pełni dopuszczalna jest sytuacja, w której dane, stanowiąc zapis informacji, mogą być źródłem różnych informacji w zależności od przyjętego przez dany podmiot sposobu ich odczytywania lub interpretacji.[117] Dane rozumiane są w analizowanym ujęciu w sposób zbliżony do informacji, w prezentowanym wyżej w niniejszym opracowaniu ujęciu substancjalnym (informacja jako wiadomość sama w sobie, określony znak, zapis, dźwięk, szyfr, kryjący pewną treść), jako określonego rodzaju znaki kulturowe, będące nośnikiem informacji.[118] Informacja natomiast oznacza rezultat procesu interpretacji danych, dokonującego się przy wykorzystaniu odpowiednich instrumentów, zdeterminowany kontekstem kulturowym oraz cechami, które indywidualizują podmiot odczytujący i interpretujący dane.[119]

[114] Informacja postrzegana jest z perspektywy semantycznej, jako określone znaczenie znaków. Podobnie kwestię tę ujmują niektórzy autorzy niemieccy, wyróżniający dwa znaczenia pojęcia informacji: semantyczne oraz syntaktyczne. Zob. J. Welp, *Datenveränderung*..., s. 443; Th. Gerhards, *Computerkriminalität*..., s. 27–28.

[115] Th. Gerhards stwierdza, że *„Die zweite Ebene des Datenbegriffes betrifft die Darstellung der Information durch Zeichen, die aufgrund einer Konvention für den Dateninhalt stehen"* (*Computerkriminalität*..., s. 29). Por. też A. Adamski, *Przestępstwa komputerowe*..., s. 27.

[116] Tak zagadnienie to ujmuje A. Adamski, powołując się na *Recomendation of the Council of the Concerning Guidelines for Security of Information Systems*, OECD/GD (92) 10, Paris 1992. Autor ten wskazuje, że Aneks do Wytycznych OECD w Sprawie Bezpieczeństwa Systemów Informacyjnych definiuje pojęcie danych w następujący sposób: „Dane (data) — przedstawienie faktów, pojęć lub poleceń w sposób sformalizowany i umożliwiający ich komunikowanie, interpretację lub przetwarzanie zarówno przez ludzi, jak i urządzenia". Informacja zaś to — wedle powyższych wytycznych — znaczenie, jakie nadajemy danym przy pomocy konwencji odnoszących się do tych danych. Zob. szerzej A. Adamski, *Przestępstwa komputerowe*..., s. 27, przyp. 27 i 28 na tej stronie.

[117] Trafnie wskazuje A. Adamski, że „wyraz składający się z takich samych liter może mieć rozmaite znaczenia w różnych językach naturalnych. Podobnie na przykład zestaw znaków numerycznych może reprezentować jakąś liczbę, literę lub znak specjalny, co odcyfrować można dopiero wówczas, gdy podmiot otrzymujący dane posiada zarazem odpowiedni klucz (oprogramowanie), pozwalający przekształcić dane (ciąg znaków) w informację o określonej treści" (*Przestępstwa komputerowe*..., s. 27–28).

[118] Podobne pojęcie danych rozumiane jest w piśmiennictwie niemieckim, gdzie odróżnia się dane oraz informacje. Wedle dominującego w literaturze poglądu: *„Daten sind zunächst alle für einen Computer verständlich codierte oder codierbare Informationen"* (W. Müller, *Aktuelle Probleme*..., s. 97). Zob. też analogiczne poglądy prezentowane przez F. Haft, *Das Zweite Gesetz*..., s. 8.

[119] Por. A. Adamski, *Przestępstwa komputerowe*..., s. 27–28.

W piśmiennictwie karnistycznym konkurują więc ze sobą co najmniej dwie propozycje terminologiczne związane ze sferą przestępczości komputerowej. W tym stanie rzeczy przystępując do analizy fenomenu przestępczości komputerowej konieczne jest oczyszczenie przedpola terminologicznego i przyjęcie jednego, wykorzystywanego w obszarze całego karnego prawa komputerowego, sposobu definiowania podstawowych pojęć. W odniesieniu do wymienionych wyżej dwóch modeli definicyjnych wydaje się, że koncepcja doszukująca się dystynkcji znaczeniowych pomiędzy pojęciem „dane" a terminem „informacja" posiada pewną przewagę nad uniformistycznym ujęciem substancjalnym. Po pierwsze, z tego względu, że stosunkowo dobrze koresponduje z przyjętą w polskim ustawodawstwie metodą regulacji, która odnosi się do nadużyć stanowiących ataki na zasoby informacyjne lub ataki na inne dobra prawne, dokonywanych przy wykorzystaniu nowoczesnych technik gromadzenia i przetwarzania danych. Z jednej strony bowiem w polskim ustawodawstwie karnym odnaleźć możemy przepisy chroniące integralność oraz prawo dysponowania informacją o określonej treści (np. art. 267 § 1 k.k.), z drugiej strony przepisy, które chronią nie tyle samą informację, ile raczej znaki wyrażające odpowiednie treści (np. art. 268 k.k.). Po drugie, rozróżnienie pomiędzy informacją a danymi zdaje się mieć pewne znaczenie dla interpretacji przepisów określających tzw. przestępstwa komputerowe. Jak trafnie wskazuje A. Adamski, „posiadanie dostępu do danych nie zawsze bowiem oznacza możliwość zapoznania się z treścią zawartych w nich informacji. Zniszczenie danych nie musi być równoznaczne ze zniszczeniem informacji. Kopiowanie danych nie jest ich zaborem".[120] Niezależnie zatem od tego, jakie dobro prawne chronione jest przez typ zaliczany do kręgu przestępstw komputerowych, dane zgromadzone na komputerowym nośniku informacji stanowią przedmiot czynności wykonawczej, albowiem to na nie skierowane są bezpośrednio działania sprawcy. Informacja zaś w zasadniczej większości przypadków przestępstw komputerowych stanowi przedmiot ochrony, który odzwierciedla główne lub poboczne dobro prawne chronione przez dany typ. Po trzecie wreszcie, ta konwencja definicyjna pozostaje w zgodzie z przyjmowanymi w aktach organizacji ponadnarodowych wzorcowymi sposobami definiowania pojęć „informacja" oraz „dane".[121] Mając na względzie przedstawione wyżej uwagi, w niniejszym opracowaniu wykorzystywane będzie ujęcie terminologiczne, które ujmuje dane jako określonego rodzaju

[120] A. Adamski, *Przestępstwa komputerowe*..., s. 28.

[121] Zob. szerzej A. Adamski, *Przestępstwa komputerowe*..., s. 27 oraz powoływany przez tego Autora Aneks do Wytycznych OECD w Sprawie Bezpieczeństwa Systemów Informacyjnych — tamże, s. 27, przyp. 27.

znaki kulturowe będące nośnikiem informacji, informację natomiast — jako rezultat procesu interpretacji danych, dokonującego się przy wykorzystaniu odpowiednich instrumentów, który jest zdeterminowany kontekstem kulturowym oraz cechami indywidualizującymi podmiot odczytujący i interpretujący dane.

V. PRZESTĘPSTWA PRZECIWKO INFORMACJI W KODEKSIE KARNYM Z 1997 R.

HACKING KOMPUTEROWY — ART. 267 § 1 K.K.

11. Przepis art. 267 § 1 k.k. określa nieznany Kodeksowi karnemu z 1969 r. typ czynu zabronionego, które penalizuje zachowania polegające na bezprawnym uzyskaniu informacji poprzez przełamanie jej szczególnego zabezpieczenia lub podłączenie się do przewodu służącego do przekazywania informacji. Zgodnie z brzmieniem tego przepisu, grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch podlega ten, „kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie". Podobny typ czynu zabronionego określony jest w § 202a niemieckiego kodeksu karnego (StGB),[122] wedle którego: „1. Kto bez upoważnienia uzyskuje dla siebie lub kogoś innego informacje, które nie są dla niego przeznaczone i zostały szczególnie zabezpieczone przed nieuprawnionym dostępem, podlega karze pozbawienia wolności do lat 3 lub grzywnie. 2. Przez informacje w rozumieniu pkt 1 rozumieć należy tylko takie informacje, które zostały zapisane lub przekazywane elektronicznie, magnetycznie lub w inny podobny sposób".[123] Normatywny charakter obu przytoczonych wyżej przepisów wykazuje daleko idące podobieństwa. Mimo iż w uzasadnieniu rządowego projektu nowego Kodeksu karnego nie wskazuje się wprost na zamiar zniwelowania luki w sferze ochrony tajemnicy informacji, zapisanej na komputerowym nośniku informacji, jako przesłankę wprowadzenia przepisu art. 267 § 1 do k.k.,[124] wydaje się uzasadnione twierdzenie, iż podstawową funkcją tego przepisu jest wypełnienie luki, jaka istniała w ochronie tajemnicy informacyjnej zakodowanej na komputerowych nośnikach informacji.[125]

Przepis art. 267 § 1 k.k., podobnie jak jego niemiecki odpowiednik, obejmuje ochroną szeroko rozumiane prawo do dysponowania informacją, mające charakter prawa podmiotowego.[126] Mimo iż bezprawne uzyskanie informacji zakodowanej na komputerowym6 nośniku występuje łącznie z charakterystyką czynności sprawczej polegającej na otwarciu zamkniętego pisma, wydaje się, iż w przypadku hackingu komputerowego ochronie podlegają nie tylko informacje dotyczące osoby, lecz wszelkie informacje zakodowane elektronicznie lub magnetycznie, podlegające ochronie na podstawie odpowied-

[122] Zestawiając ze sobą przepisy art. 267 k.k. z 1997 r. oraz § 202 a StGB podkreślić należy, iż zostały one zamieszczone w rozdziałach grupujących typy wymierzone w podobne dobra prawne (w przypadku polskiego Kodeksu karnego jest to rozdział obejmujący „Przestępstwa przeciwko ochronie informacji"; w niemieckim kodeksie karnym rozdział obejmujący przestępstwa przeciwko sferze prywatnej (tajemnicy prywatnej) oraz tajemnicy osobistej — *„Verletzung des persönlichen Lebens- und Geheimbereichs"*). Między konstrukcją obu typów zachodzą oczywiście dość istotne różnice, które stanowić będą przedmiot analizy w dalszej części niniejszego opracowania. W tym miejscu podkreślić należy jedną istotną dla interpretacji znamion odmienność między oboma typami, w ustawie karnej niemieckiej wyraźnie oddzielono od siebie naruszenie tajemnicy korespondencji (określone w § 202 StGB — *Verletzung des Briefgeheimnisses*) oraz bezprawne uzyskanie informacji zgromadzonej na elektronicznym nośniku (określone w powołanym wyżej § 202a StGB — *Ausspähen von Daten*). W polskim Kodeksie karnym przepis art. 267 obejmuje znamionami zarówno zachowania polegające na naruszeniu tajemnicy korespondencji, jak i bezprawne uzyskanie informacji zapisanej na elektronicznym nośniku.

[123] W oryginalnym brzmieniu językowym przepis ten stanowi: § 202a 1. *„Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. 2. Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar sind oder übermittelt werden."* Przepis ten znajduje się w rozdziale XV niemieckiego kodeksu karnego, pt. „Naruszenie sfery prywatności i tajemnicy osobistej" (*Verletzung des persönlichen Lebens- und Geheimbereichs*).

[124] W uzasadnieniu rządowego projektu nowego Kodeksu karnego stwierdza się jedynie, że „z ochroną informacji stanowiących cudzą tajemnicę, związaną z przestępstwami komputerowymi, polegającymi na bezprawnym pozyskiwaniu informacji przełamując elektroniczne, magnetyczne lub inne szczególne ich zabezpieczenia, niszczeniu bez uprawnienia, uszkadzaniu lub zmianie zapisu istotnej informacji na komputerowym nośniku informacji są związane typy określone w art. 267 § 1, art. 268 § 1 i 2", *Uzasadnienie rządowego projektu nowego Kodeksu karnego* (w:) *Nowe kodeksy karne — z 1997 r. z uzasadnieniami*, Warszawa 1997, s. 205. Zob. też A. Adamski, *Hacking a nowy kodeks karny*, Informatyka 1998, nr 9, s. 15 i n.

[125] Na takie *ratio legis* wskazują wyraźnie autorzy niemieccy komentujący przepis § 202a StGB. Tak m.in. T. Lenckner stwierdza, że: *„Die durch das 2. WiKG eingefügte Vorschrift soll die Strafbarkeitslücken schliessen, die mit dem Aufkommen computergestützter Informations- und Kommunikationssysteme bei § 202 entstanden waren"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1350). Zob. też U. Sieber, *Informationstechnologie...*, s. 51.

[126] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1003; R. Zakrzewski, *Przestępstwa przeciwko ochronie informacji*, Monitor Prawniczy 1998, nr 10, s. 378 i n. W odniesieniu do § 202a StGB T. Lenckner podkreśla, że: *„Entsprechend § 202 ist Rechtsgut des § 202a daher die formelle Verfügungsbefugnis desjenigen, der als Herr der Daten — d.h. kraft seines Rechts an ihrem gedanklichen Inhalt und damit unabhängig von den Eigentumsverhältnissen am Datenträger — darüber bestimmen kann, wem diese zugänglich sein sollen"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1350).

niego tytułu prawnego.[127] Chronione na mocy art. 267 § 1 k.k. prawo do dysponowania informacją swoje konstytucyjne odzwierciedlenie znajduje w treści przepisu art. 47 (ochrona prywatności) oraz art. 49, statuującego ochronę tajemnicy i swobody komunikowania się. Ma ono także odpowiedniki w przepisach prawa autorskiego, wynalazczego i patentowego. Przepis art. 267 § 1 stanowi zmodyfikowany odpowiednik przestępstwa określonego w art. 172 k.k. z 1969 r., chroniącego tajemnicę korespondencji.[128]

Spośród wymienionych w art. 267 § 1 czynności sprawczych, w kontekście analizy przestępstw komputerowych znaczenie posiadają zachowania polegające na uzyskaniu bez uprawnienia informacji poprzez „podłączenie się do przewodu służącego do przekazywania informacji" albo poprzez „przełamanie elektronicznego, magnetycznego albo innego szczególnego zabezpieczenia" tych informacji.[129] Obie formy dokonania czynności wykonawczej powiązane są bowiem z nowoczesnymi technologiami gromadzenia i przetwarzania informacji. Podłączenie się do przewodu służącego do przekazywania informacji przybierać może postać przyłączenia urządzenia odbiorczego do kabla telefonicznego, do sieci kablowej służącej do przekazywania obrazu lub do sieci komputerowej.[130] W tym ostatnim przypadku informacje uzyskiwane przez sprawcę pochodzą z komputerowej bazy danych wykorzystywanej w sieci. Można przyjąć, iż w pewnych wypadkach wykorzystanie tej formy zachowania stanowić będzie podstawę do uzyskania informacji zabezpieczonych przy pomocy specjalnych elektronicznych, magnetycznych lub innych specjalnych zabezpieczeń, które nie zostają przez sprawcę przełamane, albowiem dostęp do zabezpieczonej informacji sprawca uzyskuje na etapie jej przekazywania w obrębie sieci komputerowej poprzez przyłączenie się do przewodu służącego do przekazywania informacji. W tym sensie wymieniony sposób zachowania sprawcy stanowi przejaw ataku na informację zgromadzoną w systemie komputerowym, która standardowo jest niedostępna dla osób nie będących uprawnionymi użytkownikami systemu.

[127] Por. F. Haft, *Das Zweite Gesetz...*, s. 9 i n.; T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1350; E. Samson (w:) *Systematischer Kommentar zum Strafgesetzbuch*, Band II, *Besonderer Teil*, s. 1 i n.

[128] Artykuł 172 k.k. z 1969 r., obejmował ochroną tylko pewną kategorię informacji przed zamachami polegającymi stanowiąc w ostatniej wersji: „Kto bez uprawnienia otwiera zamknięte pismo dla niego nie przeznaczone albo ukrywa lub niszczy cudzą korespondencję, zanim adresat się z nią zapoznał, albo przyłącza się do przewodu służącego do podawania wiadomości, albo podstępnie uzyskuje nie przeznaczoną dla niego wiadomość nadaną przy użyciu środków telekomunikacji, podlega karze pozbawienia wolności do lat 2, ograniczenia wolności albo grzywny".

[129] Ta postać czynności wykonawczej nie była w ogóle przewidziana w znamionach przestępstwa określonego w art. 172 k.k. z 1969 r. Zob. przypis 127.

[130] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1005–1006.

Drugi z wymienionych powyżej sposobów zachowania się sprawcy stanowi ustawowy wyraz klasycznego przestępstwa komputerowego, określonego w literaturze karnistycznej jako tzw. hacking komputerowy.[131] Czynność sprawcza polega na uzyskaniu informacji, które poprzedzone jest przełamaniem elektronicznego, magnetycznego lub innego szczególnego ich zabezpieczenia. Ten element znamion przestępstwa określonego w art. 267 § 1 k.k. wykazuje daleko idące podobieństwo do znamion przestępstwa przewidzianego w § 202a StGB.[132] W obu typach istota zachowania karalnego sprowadza się do uzyskania przez sprawcę chronionej informacji poprzez przełamanie jej szczególnego zabezpieczenia. Elektroniczne, magnetyczne lub inne szczególne zabezpieczenia rozumieć należy w kontekście pozostałych znamion hackingu komputerowego określonych w art. 267 § 1 k.k. jako elementy, które zgodnie z wolą osoby dysponującej zakodowanymi na komputerowym nośniku informacjami mają wykluczać lub co najmniej stanowić poważne utrudnienie dostępu do tych informacji osobom nieuprawnionym. Należy podkreślić, iż zarówno polski, jak i niemiecki przepis wymaga dla realizacji znamion przełamania „szczególnych zabezpieczeń" służących do ochrony informacji przed nieuprawnionymi osobami. W piśmiennictwie niemieckim podkreśla się, iż hacking komputerowy możliwy jest jedynie wówczas, gdy zakodowane na specjalnym nośniku informacje są rzeczywiście szczególnie zabezpieczone, przy czym nie jest konieczne, aby odpowiednie elektroniczne, magnetyczne lub inne specjalne mechanizmy służyły wyłącznie zabezpieczeniu informacji, jednak funkcja zabezpieczająca musi pełnić w takim przypadku zasadniczą, dominującą rolę.[133]

[131] Zob. U. Sieber, *Przestępczość komputerowa...*, s. 227–228; A. Adamski, *Przestępstwa komputerowe...*, s. 39–41; E. Czarny–Drożdżejko, *Ochrona informacji i programów komputerowych* (w:) *Prawo autorskie a postęp techniczny*, red. J. Barta, R. Markiewicz, Kraków 1999, s. 200–202; K.J. Jakubski, *Przestępczość komputerowa — zarys...*, s. 47 i n.

[132] Przepis ten w ust. 1 zawiera znamię „szczególnego zabezpieczenia dostępu do informacji" (*„gegen unberechtigten Zugan besonders gesichert sind"*), natomiast w ust. 2 wyraźnie określa, iż owo szczególne zabezpieczenie dotyczyć może jedynie informacji zakodowanych (zapisanych) elektronicznie, magnetycznie lub w inny sposób, uniemożliwiający ich bezpośrednie dostrzeganie. Powiązanie ze sobą obu ustępów § 202a StGB pozwala stwierdzić, iż także na gruncie tego przepisu szczególne zabezpieczenie to m.in. zabezpieczenie elektroniczne lub magnetyczne. W piśmiennictwie jako klasyczne przykłady zabezpieczeń wymienia się hasła, numery identyfikacyjne, karty magnetyczne, dekodery palcowe lub głosowe; T. Lenckner podkreśla, że należą tutaj w szczególności *„Passworte, Benutzerkennummern, Magnetkarten, Fingerabdruck- und Stimmerkennungsgeräte"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1352).

[133] T. Lenckner podkreśla, że: *„Gegen unberechtigten Zugang besonders gesichert sind się, wenn Vorkehrungen getroffen sind, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf die Daten auszuschliessen oder wenigstens nicht unerheblich zu erschweren. Dies braucht zwar nicht ihr einziger Zweck zu sein, jednefalls aber muss der Berechtigte durch die Sicherung gerade auch sein spezielles Interesse an der Geheimhaltung dokumentieren"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1352).

Pogląd ten można, jak się wydaje, recypować na grunt art. 267 § 1 k.k. Należy zaznaczyć, że elektroniczne, magnetyczne lub inne szczególne zabezpieczenie może odnosić się bezpośrednio do określonych zasobów informacji (np. plików w zbiorach komputerowych), może jednak także służyć ochronie całego systemu lub sieci albo urządzeń służących do jego obsługi.[134] W tym drugim wypadku dane zgromadzone w systemie lub sieci chronione są w sposób szczególny niejako pośrednio, co jednak w niczym nie zmienia faktu, iż mamy wówczas do czynienia ze spełnieniem warunku szczególnego zabezpieczenia informacji.[135] W piśmiennictwie niemieckim podkreśla się także — a teza ta z pewnością może być rozciągnięta na polski art. 267 § 1 k.k. — że dla realizacji znamion hackingu konieczne jest rzeczywiste funkcjonowanie zabezpieczeń informacji w czasie ataku dokonywanego przez osobę nieuprawnioną.[136] Oznacza to, iż samo zainstalowanie specjalnych zabezpieczeń informacji nie wystarcza dla realizacji znamion przestępstwa hackingu, konieczne jest bowiem, aby w chwili działania sprawcy zabezpieczenie było aktywne i w konsekwencji zostało przez sprawcę przełamane.

W związku z tak określonym znamieniem czynności wykonawczej, w piśmiennictwie pojawiają się pewne wątpliwości dotyczące najbardziej typowej postaci hackingu, polegającej na uzyskaniu informacji poprzez wdarcie się sprawcy do systemu komputerowego dokonane poprzez pokonanie zainstalowanych w systemie odpowiednich zabezpieczających kodów i haseł.[137] Kryminalizacja tego rodzajów nielegalnych sposobów uzyskania informacji zgromadzonych na komputerowym nośniku wywołuje wiele kontrowersji

[134] Odnoszące się do problematyki szczególnego zabezpieczenia danych zgromadzonych na komputerowych nośnikach informacji rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 80, poz. 521), w § 1 pkt 2 stanowi, że przez zabezpieczenie systemu informatycznego „rozumieć należy wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą".

[135] Odnosząc się do tego zagadnienia T. Lenckner pisze: *„Zugangssicherungen bei gespeicherten Daten sind nicht nur solche, die unmittelbar am Datenspeicher oder gar am Datum selbst angebracht sind, vielmehr genügen auch mittelbare Sicherungen in der Weise, dass das zum Abruf der Daten notwendige Betriebssystem gesichert oder das Datenverarbeitungszentrum als «Closed–shop» betrieben wird"* — w: Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1352. Zob. też E. Samson w: *Systematischer Kommentar...*, s. 10; H. Tröndle, *Strafgesetzbuch und Neengesetze*, 48. Auflage, München 1997, s. 275.

[136] T. Lenckner (w:) Schönke/Schröder, *Strefgesetzbuch. Kommentar...*, s. 1352.

[137] Zob. T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1351; E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 198–199.

w piśmiennictwie karnistycznym.[138] Zwolennicy bezkarności tego rodzaju zachowań podnoszą, że w wielu wypadkach, być może stanowiących nawet zasadniczą większość przypadków tzw. hackingu, sprawcy nie podejmują czynności w celu wyrządzenia szkody dysponentowi informacji ani też w celu zdobycia tej informacji dla siebie, lecz działają jedynie w celu sprawdzenia swoich możliwości przełamania zainstalowanych przez użytkownika systemu specjalnych systemów zabezpieczających.[139] Rostrzygnięcie zagadnienia karalności tego rodzaju zachowań na podstawie art. 267 § 1 k.k. wymaga odniesienia się do przyjmowanych w różnych ustawodawstwach karnych metod kryminalizacji hackingu.

Z punktu widzenia techniki legislacyjnej oraz zakresu prawnokarnej ochrony wyróżnić można trzy modele kryminalizacji zachowań hackerów. Pierwszy, ujmujący najszerzej zakres ochrony, polega na wprowadzeniu kryminalizacji samego przełamania zabezpieczenia i wdarcia się przez sprawcę do systemu. W tym ujęciu nie jest istotny cel działania sprawcy ani też fakt uzyskania przez niego dostępu lub wręcz zdobycia zgromadzonych w systemie informacji. Taki sposób kryminalizacji przełamania zabezpieczeń systemów komputerowych oparty jest na konstrukcji przestępstwa narażenia na niebezpieczeństwo informacji zgromadzonych w systemie.[140] W drugim modelu karalne jest wdarcie się sprawcy do systemu komputerowego w celu uzyskania zgromadzonych w nim informacji.[141] Krąg zachowań karalnych ograniczony jest tutaj poprzez ujęcie strony podmiotowej, wymagające kierunkowego nastawienia działania sprawcy na uzyskanie zgromadzonych w systemie informacji. Także ta odmiana przestępstwa ma charakter formalny, z tym jednak, iż zakres zachowań karalnych jest tutaj zawężony poprzez wprowadzenie dodatkowego warunku podmiotowego, wymagającego działania sprawcy ze szczególną postacią zamiaru bezpośredniego, przesądzającą o kierunkowym

[138] Zob. szerzej U. Sieber, *Przestępczość komputerowa...*, s. 225; tenże, *Computerkriminalität...*, s. 45 i n.

[139] Klasyczny hacking polega na wtargnięciu do obcego systemu komputerowego, które następuje nie w celu manipulacji, sabotażu lub szpiegostwa, lecz dla uzyskania satysfakcji wynikającej z pokonania środków zabezpieczenia technicznego; zob. U. Sieber, *Przestępczość komputerowa...*, s. 227.

[140] A. Marek uznaje przestępstwo określone w art. 267 k.k. za przestępstwo „polegające na narażeniu (abstrakcyjnym) na niebezpieczeństwo sfery prywatności człowieka oraz tajemnicy korespondencji i innych form komunikowania się" (*Komentarz do Kodeksu karnego. Część szczególna*, Warszawa 2000, s. 275).

[141] Takie rozwiązanie przyjęte zostało w brytyjskiej ustawie o nadużyciach komputerowych (Computer Misuse Act), uznającej za przestępstwo samo podjęcie czynności zmierzających do uzyskania nieuprawnionego dostępu do systemu komputerowego; zob. szerzej w tej kwestii A. Adamski, *Przestępstwa komputerowe...*, s. 49; M. Wasik, *Crime and Computer*, Oxford 1991, s. 80 i n.; M. Kolecki, *Przestępstwa komputerowe...*, s. 57 i n.

charakterze tego przestępstwa.[142] Wreszcie, wedle trzeciego modelowego rozwiązania, karalne jest wdarcie się do systemu poprzedzone przełamaniem zainstalowanych w nim specjalnych zabezpieczeń, któremu towarzyszy uzyskanie przez sprawcę informacji zawartych w systemie. Ta odmiana hackingu ma charakter przestępstwa materialnego, którego znamiona wymagają wejścia sprawcy w posiadanie informacji znajdujących się w systemie.[143] Polski ustawodawca rozwiązanie zawarte w art. 267 § 1 k.k. oparł na trzecim z wymienionych wyżej modeli, czyniąc z hackingu przestępstwo, którego istotą jest uzyskanie przez sprawcę chronionej informacji.[144] Elementami charakteryzującymi zachowanie karalne są: przełamanie specjalnego zabezpieczenia informacji oraz uzyskanie bez uprawnienia informacji zabezpieczonej. Podobnie konstrukcję hackingu ujęto w § 202a niemieckiego kodeksu karnego (StGB), wymagając dla odpowiedzialności karnej przełamania szczególnego zabezpieczenia informacji oraz uzyskania (*verschaffen*) tej informacji dla sprawcy lub innej osoby.[145]

Znamię czynnościowe „uzyskuje" na gruncie wykładni językowej rozumieć należy jako przejęcie przez sprawcę władztwa nad informacją. Wedle ujęcia słownikowego „uzyskiwać" to „otrzymać zwykle coś pożądanego, coś, co było przedmiotem starań, osiągnąć, zdobyć". Czasownik „uzyskiwać" występuje najczęściej w zwrotach „uzyskać aprobatę, uzyskać pomoc, przebaczenie, pożyczkę, pracę, dyplom, stopień naukowy, dobre wyniki lub rezultaty, przewagę nad kimś, informację o czymś".[146] Uzyskanie informacji to

[142] Co do pojęcia „przestępstwo kierunkowe" oraz technicznolegislacyjnych sposobów opisywania znamion strony podmiotowej tej odmiany deliktu — zob. szerzej S. Frankowski, *Przestępstwa kierunkowe w teorii i praktyce*, Warszawa 1970, passim.

[143] Co do modeli kryminalizacji hackingu zob. szerzej E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 199. Zob. też N. Bończoszek, *Wykrywanie przestępstw komputerowych w Zjednoczonym Królestwie* (w:) *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, red. A. Adamski, Toruń 1994, s. 105 i n.

[144] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1006 i n.; E. Czarny–Drożddżejko, *Ochrona informacji...* s. 201; A. Adamski, *Przestępstwa komputerowe...*, s. 41; O. Górniok (w:) O. Górniok, S. Hoc, S.M. Przyjemski, *Kodeks karny. Komentarz*, t. III, Gdańsk 1999, s. 322–323; J. Wojciechowski, *Kodeks karny. Komentarz*. Orzecznictwo, Warszawa 1997, s. 469–470; L. Gardocki, *Prawo karne*, Warszawa 1999, s. 291 i n.; A. Marek, *Prawo karne. Zagadnienia teorii i praktyki*, Warszawa 1997, s. 468; tenże, *Komentarz do Kodeksu karnego. Część szczególna*, Warszawa 2000, s. 274–276.

[145] *„Die Tathandlung besteht darin* — podkreśla T. Lenckner — *dass der Täter die Daten sich oder einem anderen verschafft, wobei dies, wie sich aus dem Sinnzusammenhang ergibt, unter Überwindung der Zugangssicherung erfolgen muss. Verschafft sind die Daten zunächst, wenn der Täter bzw. der Dritte durch optische bzw. akkustische Wahrnehmung von ihrem Inhalt tatsächlich Kenntnis genommen hat"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1353).

[146] *Słownik języka polskiego...*, s. 598.

zatem zdobycie nad nią władztwa przez sprawcę, zdobycie możliwości jej swobodnego wykorzystywania, decydowania o jej przeznaczeniu. Może ono przejawiać się objęciem we władanie nośnika, na którym zapisana jest informacja, skopiowaniem zapisu informacji lub zapoznaniem się z jej treścią bez obejmowania władztwa nad nośnikiem, na którym jest ona zapisana. Konstytutywne dla znamion przestępstwa hackingu z art. 267 § 1 k.k. uzyskanie informacji oznacza zatem każdą formę przejęcia przez sprawcę władztwa nad informacją. Może ono polegać na objęciu w posiadanie nośnika pierwotnego (np. dyskietki komputerowej) lub na skopiowaniu informacji na inny nośnik albo zapoznaniu się z informacją na pierwotnym nośniku bez zaboru tego nośnika ani też sporządzenia kopii. Należy podkreślić, że użyte w opisie znamion przestępstwa z art. 267 § 1 k.k. pojęcie „uzyskanie" nie jest synonimem terminu „zapoznanie się[147] z informacją". Zapoznanie się z treścią informacji stanowi tylko jedną z możliwych form realizacji znamion przestępstwa hackingu. W wypadku gdy zachowanie sprawcy polega na objęciu przez sprawcę władztwa nad nośnikiem, na którym zapisana jest informacja, wówczas sam ten fakt przesądza o uzyskaniu przez niego informacji w rozumieniu art. 267 § 1 k.k. Dla spełnienia tego elementu znamion nie jest w takim przypadku konieczne rzeczywiste zapoznanie się sprawcy z treścią informacji,[148] ani też nawet istnienie po jego stronie obiektywnej możliwości rozumienia tej informacji.[149] Warunkiem wypełnienia tego elementu znamion jest, aby osoba przełamująca zabezpieczenie i uzyskująca informację nie była do tego upraw-

[147] W ujęciu słownikowym „zapoznać się — zapoznawać się" oznacza „poznać coś dokładnie, posiąść wiedzę o kimś, o czymś, dojść d znajomości czegoś" (*Słownik języka polskiego...*, s. 885).

[148] Podobnie R. Zakrzewski, stwierdzając, że „przestępstwa z art. 267 i art. 268 k.k. uważać należy za dokonane z chwilą dopuszczenia się jednego z zakazanych działań bez względu na to, czy sprawca zapoznał się z treścią nie przeznaczonej dla niego informacji" (*Przestępstwa przeciwko ochronie informacji...*, s. 378). Identycznie tenże, *Ochrona informacji w nowym kodeksie karnym*, Przegląd Ustawodawstwa Gospodarczego 1998, nr 10, s. 13. W podobnym duchu, acz niejednoznacznie, zdaje się wypowiadać w tej kwestii O. Górniok (w:) *Kodeks karny...*, s. 322–323. Zob. też J. Wojciechowski, *Kodeks karny. Komentarz. Orzecznictwo*, Warszawa 1997, s. 469; A. Marek; *Prawo karne. Zagadnienia teorii i praktyki*, wyd. 2, Warszawa 2000, s. 685–686; L. Gardocki, *Prawo karne...*, s. 291; W. Świda (w:) I. Andrejew, W. Świda, W. Wolter, *Kodeks karny z komentarzem*, Warszawa 1973, s. 504–505.

[149] Identycznie W. Wróbel, *Uwagi wprowadzające...*, s. 1004. Odmiennie A. Adamski, zdaniem którego „przestępstwo z art. 267 § 1 k.k. jest przestępstwem materialnym. Jego karalnym skutkiem jest zapoznanie się przez sprawcę z treścią zastrzeżonej dla niego informacji" (*Przestępstwa komputerowe...*, s. 40–41). W innym zaś miejscu tego samego opracowania Autor ten stwierdza, że „należy przyjąć, że samo skopiowanie przez sprawcę plików danych zawierających informacje, z którymi nie zdążył się on jeszcze zapoznać nie wyczerpuje znamion ustawowych omawianego przestępstwa" (*Przestępstwa komputerowe...*, s. 42). Identycznie tenże, *Karalność hackingu...*, s. 149 i n.

niona.[150] Użyte w treści art. 267 § 1 k.k sformułowanie „bez uprawnienia" pełni w tym przepisie funkcję klauzuli normatywnej.[151] Przepisy prawa karnego, w tym także sam art. 267 k.k., nie przesądzają o tym, kto posiada uprawnienie do uzyskiwania określonego rodzaju informacji. Rozstrzygnięcie tej kwestii dokonywane być musi w oparciu o inne, pozakarne regulacje, odnoszące się do sfery uprawnień poszczególnych podmiotów do uzyskiwania określonego rodzaju informacji. W kontekście znamion określonych w art. 267 § 1 k.k., najistotniejsze z punktu widzenia elementu ujętego jako brak uprawnienia sprawcy do uzyskania określonych informacji jest to, aby zgodnie z wolą i kompetencją podmiotu uprawnionego do dysponowania tą informacją, w chwili czynu nie była ona legalnie dostępna dla sprawcy.[152] Co do przesłanek określających osoby uprawnione do uzyskania informacji, Kodeks karny ma ewidentnie charakter subsydiarny, chroniąc zakazy uzyskiwania określonego rodzaju informacji przez pewne kategorie podmiotów, wyrażone w innych działach prawa, regulujące zagadnienia prawa do informacji zarówno w aspekcie majątkowym, jak i niemajątkowym.[153]

Pewne wątpliwości wywołuje w literaturze zagadnienie przedmiotu, który uzyskać ma sprawca hackingu. Przepis art. 267 § 1 k.k. dla realizacji znamion wymaga, aby sprawca uzyskał informację, do której nie jest uprawniony. W przypadku klasycznych postaci tego przestępstwa (np. otwarcie zamkniętego pisma) jest oczywiste, że informacja uzyskiwana przez sprawcę stanowi odrębny przedmiot od zabezpieczenia tej informacji. Tymczasem w odniesieniu do hackingu komputerowego w literaturze podkreśla się, że dostęp do informacji znajdującej się w systemie komputerowym zasadniczo zabezpieczany jest obecnie poprzez wprowadzenie odpowiedniego hasła dostępu. Zabezpieczenie zgromadzonych w systemie informacji ma więc co do zasady charakter cyfrowy, jego treść stanowi sama w sobie *sui generis* informację.[154] „Przełamanie tego zabezpieczenia, na przykład przy użyciu specjalnego programu komputerowego służącego do odgadywania haseł — podkreśla A. Adamski — nie jest jednak odpowiednikiem rozerwania zapieczętowanej koperty przez osobę nie będącą adresatem znajdującego się w niej pisma. Łamiąc zabezpieczenie w postaci hasła, hacker często zapoznaje się z nieprzeznaczoną dla niego informacją, jaką jest treść hasła. Jeżeli tak się dzieje — zachowanie sprawcy wyczerpuje znamiona ustawowe przestępstwa z art. 267 § 1 k.k."[155] W powyższym rozumowaniu odcyfrowanie przez sprawcę treści hasła zabezpieczającego jest traktowane jako uzyskanie informacji, do zdobycia której sprawca nie jest uprawniony.[156] Tym samym, podlegająca ochronie na mocy analizowanego przepisu informacja zostaje utożsamiona z zabezpieczeniem. W alternatywnym modelu interpretacyjnym, zaproponowanym przez W. Wróbla, dla odpowiedzialności za dokonanie przestępstwa hackingu konieczne jest przesądzenie koniunktywnie dwóch okoliczności: po pierwsze tego, że sprawca wdarł się do systemu przełamując specjalne zabezpieczenie; po drugie, że konsekwencją tej czynności było uzyskanie przez niego znajdującej się w systemie informacji, różnej od treści hasła zabezpieczającego (np. cudzej korespondencji elektronicznej).[157] Pierwszy z przedstawionych modeli interpretacyjnych znamion przestępstwa z art. 267 § 1 k.k., autorstwa A. Adamskiego, wyraźnie nawiązuje do międzynarodowych standardów w zakresie penalizacji hackingu, kładących szczególny nacisk na ochronę systemów komputerowych przed nieuprawnionym dostępem do znajdujących się w nich danych; wzmacnia również funkcję ochronną analizowanego przepisu.[158] Jednak należy pamiętać, że takie rozumienie hackingu prze-

[150] Nieco inaczej ten element znamion wykładany jest w piśmiennictwie niemieckim na gruncie § 202a StGB, gdzie wymaga się posiadania przez sprawcę możliwości odczytania tej informacji, na przykład dzięki dysponowaniu przez niego odpowiednim kluczem, kodem dostępu itp. T. Lenckner tak ujmuje tę kwestię: *„Sind die Daten durch ihre Verschlüsselung besonders gesichert, so ist allerdings zu beachten, dass sie erst mit der Überwindung der Zugangssicherung, d.h. also der Entschlüsselung der Daten, verschafft sind; bei § 202a genügt noch nicht, dass der Täter eine Diskette mit verschlüsseltem Text in seine Verfügungsgewalt bringt, vielmehr liegt ein Verschaffen hier erst vor, wenn er die Daten tatsächlich entschlüsselt hat oder jedenfalls auch den Schlüssel in seinen Besitz bringt. Noch kein Verschaffen ist auch das blosse Eindringen in einen Datenspeicher oder Datenübermittlungsvorgang. Von § 202a nicht erfasst ist daher — entgegen ursprünglich weitergehenden Vorschlägen — das sog. Hacking, das sich im blossen Knacken eines Computersystems erschöpft"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar*..., s. 1353). Zob. też identycznie brzmiące tezy, H. Töndle, *Strafgesetzbuch*..., s. 254 i n.; E. Samson (w:) *Systematischer Kommentar*..., s. 9.

[151] Zob. szerzej co do pojęcia „klauzula normatywna" w prawie karnym — W. Wolter, *Klauzule normatywne w przepisach karnych*, Krakowskie Studia Prawnicze 1969, R. II, z. 3–4, s. 5–37; Z. Ćwiąkalski, *Znamiona normatywne w kodeksie karnym* (w:) *Problemy odpowiedzialności karnej. Księga ku czci Prof. K. Buchały*, Kraków 1994, s. 19 i n.; T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar*..., s. 1351.

[152] Por. T. Lenckner, który podkreśla, że *„für den Täter nicht bestimmt sind die Daten, wenn sie ihm nach dem Willen des Berechtigten im Zeitpunkt der Tathandlung nicht zur Verfügung stehen sollen"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar*..., s. 1351).

[153] Zob. W. Wróbel, *Uwagi wprowadzające*..., s. 1003; E. Czarny–Drożdżejko, *Ochrona informacji*..., s. 200–201.

[154] Zob. A. Adamski, *Przestępstwa komputerowe*..., s. 39.

[155] *Ibidem*, s. 39.

[156] A. Adamski stwierdza jednoznacznie, że „na skutek przełamania zabezpieczenia, np. przy użyciu programu służącego do odgadywania haseł, hacker zapoznaje się z nieprzeznaczoną dla niego informacją, jaką jest treść hasła" (*Karalność hackingu*..., s. 151–152).

[157] Zob. W. Wróbel, *Uwagi wprowadzające*..., s. 1007. Podobnie interpretowane jest przepis § 202a niemieckiego kodeksu karnego w piśmiennictwie niemieckim. Zob. w tej kwestii T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar*..., s. 1352–1353.

[158] Por. A. Adamski, *Karalność hackingu*..., s. 152.

kształca to przestępstwo w typ, którego istotą staje się karalność samego uzyskania przez nieuprawnionego sprawcę dostępu do systemu komputerowego w wyniku przełamania zabezpieczeń.[159] A. Adamski podkreśla, że w proponowanym przez niego ujęciu hacking staje się typem zbliżonym do przestępstwa naruszenia miru domowego.[160] Recepcję tej koncepcji interpretacyjnej na grunt polskiego k.k. z 1997 r. uniemożliwia kształt znamion przestępstwa hackingu, które wymagają z jednej strony przełamania przez sprawcę specjalnego zabezpieczenia służącego ochronie dostępu do informacji, jaka znajduje się na nośniku komputerowym, z drugiej zaś — uzyskania tej informacji przez sprawcę.[161] Ewidentnie także w odniesieniu do hackinu art. 267 § 1 k.k. rozróżnia zabezpieczenie, służące zamknięciu osobom nieuprawnionym dostępu do informacji, oraz samą informację podlegającą zabezpieczeniu.[162] Tego rozróżnienia nie mogą zniwelować specjalne właściwości zabezpieczeń elektronicznych, które powodują, iż także zabezpieczenie w istocie składa się z odpowiedniej, z założenia niedostępnej dla sprawcy informacji (np. treść hasła dostępu). W tym kontekście konstrukcja przestępstwa hackingu wykazuje pewne podobieństwo do konstrukcji przestępstwa kradzieży z włamaniem.[163] Warunkiem koniecznym realizacji znamion typu określonego w art. 267 § 1 k.k. jest więc zawsze przesądzenie dwóch elementów: po pierwsze, faktu przełamania przez sprawcę zabezpieczenia informacji, po drugie, uzyskania tej specjalnie zabezpieczanej informacji.[164] Stąd też należy przyjąć, że samo przełamanie zabezpieczenia, nie powiązane z uzyskaniem przez

[159] Krytycznie o takim modelu kryminalizacji pisze T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1353; H. Tröndle, *Strafgesetzbuch...*, s. 253 i n.; T. Lenckner, R. Winkelbauer, *Computerkriminalität...*, s. 488 i n.

[160] A. Adamski, *Przestępstwa komputerowe...*, s. 41–42. Autor ten wskazuje, że niektóre ustawodawstwa zachodnie charakteryzują przestępstwa hackingu właśnie jako typ zbliżony do konstrukcji naruszenia miru domowego — tak np. k.k. Holandii (art. 138a) oraz Finlandii (art. 8 w rozdziale 8 k.k.).

[161] Podobnie wypowiada się w tej kwestii O. Górniok stwierdzając, że „przestępstwo jest dokonane wraz z uzyskaniem informacji (jakiejkolwiek, nie musi to być informacja, której poszukiwał) zabezpieczonej w sposób, o którym tu mowa" (w: *Kodeks karny...*, s. 323). Zob. też W. Wróbel, *Uwagi wprowadzające...*, s. 1007; L. Gardocki, *Prawo karne...*, s. 291.

[162] Przepis ten z jednej strony wprowadza karalność nie uprawnionego uzyskania informacji nieprzeznaczonej dla sprawcy („kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną"), z drugiej określa normatywne warunki karalności, wymagając, aby uzyskanie takiej informacji następowało w wyniku „przełamania elektronicznego, magnetycznego albo innego szczególnego jej zabezpieczenia". Treść art. 267 § 1 k.k. jednoznacznie rozstrzyga, że informacja jest czymś kategorialnie różnym od zabezpieczenia. Podobnie jest na gruncie § 202a StGB — zob. szerzej T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1351–1353.

[163] Zob. A. Adamski, *Przestępstwa komputerowe...*, s. 42.

[164] Por. T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1351–1353; F. Haft, *Das Zweite Gesetz...*, s. 6 i n.

sprawcę informacji, która była przez to zabezpieczenie chroniona, nie stanowi realizacji znamion przestępstwa hackingu w rozumieniu art. 267 § 1 k.k.,[165] lecz jedynie usiłowanie popełnienia tego typu, o ile sprawcy można przypisać zamiar uzyskania informacji.[166]

Drugi z elementów charakteryzujących zachowanie sprawcy to przełamanie elektronicznego, magnetycznego lub innego szczególnego zabezpieczenia. Pojęcie „przełamanie" interpretować należy w kontekście pozostałych znamion omawianego typu czynu zabronionego, jako zachowanie polegające na zniwelowaniu istniejących, specjalnych konstrukcji, których podstawową funkcją jest uniemożliwienie dostępu osobom nieuprawnionym do informacji zgromadzonych w systemie.[167] Należy podkreślić, iż w treści art. 267 § 1 k.k. zabezpieczenie powiązane zostało z informacją, co oznacza, że chodzi tutaj o takie konstrukcje, których celem jest ochrona dostępu do samej informacji. Zabezpieczenia rozumiane być winny jako wszelkiego rodzaju konstrukcje uniemożliwiające lub utrudniające dostęp do informacji, których usunięcie wymaga od sprawcy specjalistycznej wiedzy albo dysponowania specjalistycznymi urządzeniami. Z punktu widzenia konstrukcji przestępstwa hackingu nie jest istotna technologiczna strona zabezpieczeń. O tym, czy konkretny rodzaj zabezpieczenia wykorzystany do ochrony zgromadzonych w systemie informacji ma charakter elektroniczny, czy magnetyczny, decydują jego właściwości technologiczne. Doprecyzowanie istoty obu tych rodzajów zabezpieczeń ma pewne znaczenie dla interpretacji klauzuli dopełniającej, wyrażonej w art. 267 § 1 k.k. *in fine* w sformułowaniu „albo inne szczególne jej zabezpieczenie". Wydaje się bowiem, że ta trzecia niedookreślona postać zabezpieczenia wymaga co najmniej tego, aby z konstrukcyjnego punktu widzenia jej przełamanie sprawiało sprawcy trudność w takim samym stopniu, jak przełamanie zabezpieczenia elektronicznego lub magnetycznego. Pewne wątpliwości podniesione zostały w piśmiennictwie w odniesieniu do samego pojęcia „przełamanie". Z jednej bowiem strony obejmuje ono z całą pewnością zarówno takie sytuacje, w których sprawca usuwa istniejące zabezpie-

[165] Identycznie jest w przypadku przestępstwa określonego w § 202a StGB — por. T. Lenckner (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1353. Odmiennie stanowisko w tej kwestii zajmuje Bühler, *Ein Versuch...*, s. 453.

[166] Por. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 201; W. Wróbel, *Uwagi wprowadzające...*, s. 1007.

[167] Istota zabezpieczenia informacji jest analogiczna do istoty zabezpieczenia przełamywanego przez sprawcę w przypadku kradzieży z włamaniem. Zob. szerzej w tej kwestii M. Dąbrowska–Kardas, P. Kardas (w:) G. Bogdan, K. Buchała, Z. Ćwiąkalski, M. Dąbrowska–Kardas, P. Kardas, J. Majewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel, A. Zoll, *Kodeks karny. Część szczególna. Komentarz*, t. 3, Kraków–Zakamycze 1999, s. 49–53.

czenie, na przykład niszcząc je, z drugiej — rozciąga się także na wypadki, w których sprawca oddziałuje bezpośrednio na zabezpieczenie, lecz nie dokonuje jednocześnie jego zniszczenia, niwelując jedynie na pewien czas jego funkcję zabezpieczającą. Oba wymienione przypadki nie wywołują poważniejszych trudności, każdy z nich stanowi bowiem przejaw złamania bariery chroniącej dostęp do informacji, jest więc przełamaniem zabezpieczenia.[168] Kłopotliwa na gruncie znamion hackingu z art. 267 § 1 k.k. jest natomiast sytuacja, w której sprawca w ogóle nie oddziałuje bezpośrednio na istniejące zabezpieczenie informacji, lecz dokonuje jedynie jego „obejścia", wykorzystując istniejącą obok zainstalowanego zabezpieczenia strefę dostępu do informacji.[169] Wątpliwości związane z taką formą zachowania sprawcy potęgują się tym bardziej, że klasyczna formuła hackingu sprowadza się właśnie nie tyle do przełamania zabezpieczenia, co raczej do jego obejścia, a zatem stworzenia możliwości dojścia do informacji poprzez ścieżkę dostępu nieobjętą zabezpieczeniem. Posłużenie się przez ustawodawcę w znamionach przestępstwa z art. 267 § 1 k.k. pojęciem „przełamanie" zdaje się ograniczać zakres zastosowania tego przepisu. Przełamanie zabezpieczenia — powtórzmy to raz jeszcze — to wedle językowej wykładni wpływanie lub oddziaływanie przez sprawcę na funkcjonowanie zabezpieczenia w sposób, który doprowadza do zniwelowania podstawowej funkcji zabezpieczenia i otwiera sprawcy dostęp do informacji.[170] Jednoznacznie czynność przełamywania skierowana musi być na zabezpieczenie. W przypadku oddziaływania sprawcy na charakterystyczne dla systemów komputerowych zabezpieczenia elektroniczne, mające postać specjalnych haseł dostępu, kodów, specjalnych programów komputerowych itp., zachowanie sprawcy (hakera) przyjmuje postać czynności wyszukiwawczych, otwierających drogę do systemu.[171] Zawsze jednak, niezależnie od stosowanej przez sprawcę techniki, jego działanie skierowane być musi na funkcjonowanie zabezpieczenia i zmierzać do uzyskania dostępu do zabezpieczonej informacji. W literaturze wskazuje się, że ta postać czynności wykonawczej wykazuje podobieństwo do charakterysty-

[168] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1006–1007; O. Górniok (w:) *Kodeks karny...*, s. 323.

[169] W. Wróbel stwierdza w odniesieniu do tej kwestii, że przełamanie zabezpieczenia następuje wyłącznie wówczas, gdy sprawca swoim działaniem wpływa na funkcjonowanie tego zabezpieczenia. Jeżeli istnieje taki sposób dostępu do informacji, który nie został objęty szczególnym zabezpieczeniem, to skorzystanie z tego sposobu nie stanowi realizacji znamion z art. 267 § 1 k.k., choćby nawet osobie zapoznającej się z informacjami wiadoma była wola ich zabezpieczenia przed osobami postronnymi" (*Uwagi wprowadzające...*, s. 1007).

[170] Podobnie zagadnienie to ujmuje W. Wróbel, *Uwagi wprowadzające...*, s. 1007.

[171] Por. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 201.

ki włamania opisanej w art. 279 k.k.[172] Niektórzy autorzy określają ją nawet mianem „włamania komputerowego".[173] Wykładnia tego znamienia wskazuje jednoznacznie na konieczność oddziaływania sprawcy na zabezpieczenie w celu uzyskania dojścia do zablokowanego przez nie dostępu do informacji. Stąd też wszelkie zachowania otwierające sprawcy drogę do informacji zgromadzonych w systemie komputerowym, które nie stanowią oddziaływania na zabezpieczenie, lecz sprowadzają się do wyszukania przez sprawcę drogi dojścia do informacji niejako „obok" zabezpieczenia (obejścia), nie stanowią realizacji znamion przestępstwa określonego w art. 267 § 1 k.k., nawet jeżeli sprawca uzyskuje zgromadzone w systemie informacje, nie mając do tego uprawnienia. W szczególności wypełnia znamion przestępstwa określonego w art. 267 § 1 k.k. uzyskanie informacji dzięki stosowaniu metody tzw. inżynierii społecznej (*social engineering*), polegającej na wprowadzeniu dysponenta poszukiwanej przez hackera informacji w błąd co do tożsamości i uzyskanie od niego informacji umożliwiających wejście do systemu bez potrzeby forsowania zabezpieczeń.[174] W tych wypadkach sprawca nie przełamuje zabezpieczenia, lecz wykorzystując podstępnie zdobyty klucz dojścia dostaje się do systemu. Podobnie nie stanowi przestępstwa z art. 267 § 1 k.k. wykorzystanie przez sprawcę luki (*bug*) w istniejących zabezpieczeniach[175] ani też zastosowanie przez sprawcę techniki polegającej na przechwyceniu sesji legalnego użytkownika (*session hijacking*). Istota zachowania sprawcy stosującego tę technikę sprowadza się do „podszycia się" pod uprawnionego użytkownika systemu i uzyskania w trakcie przekazywania niedostępnych dla sprawcy informacji.[176]

Natomiast za wypełnienie znamion przestępstwa hackingu uznać należy uzyskanie informacji przy wykorzystaniu techniki *IP spoofing*, która polega na przerobieniu adresów w sposób uniemożliwiający ich rozpoznanie przez mechanizmy zabezpieczające system. Dzięki temu zabiegowi sprawca unika

[172] Takie ujęcie przestępstwa z art. 267 § 2 k.k. jest krytykowane w doktrynie. A. Adamski stwierdza, że „typizacja hackingu wzorowana na konstrukcji przestępstwa kradzieży z włamaniem jest wadliwa i pomimo stosowania intensywnych zabiegów interpretacyjnych nie jest w stanie zapewnić odpowiedniego standardu ochrony prawnej dostępności, poufności i integralności elektronicznie przetwarzanej informacji" (*Przestępstwa komputerowe...*, s. 49); tenże, *Karalność hackingu...*, s. 149 i n. Zob. też omówienie projektowanych modeli odpowiedzialności za hacking w Wielkiej Brytanii M. Wasik, *Crime and the Computer*, Oxford 1991, s. 80 i n.

[173] Tak m.in. O. Górniok (w:) *Kodeks karny...*, s. 323. Podobne stanowisko zajmują w odniesieniu do znamion przestępstwa z art. 279 k.k. M. Dąbrowska–Kardas i P. Kardas (w:) *Kodeks karny. Część szczególna...*, s. 53.

[174] A. Adamski, *Karalność hackingu...*, s. 153–154.

[175] A. Adamski, *Karalność hackingu...*, s. 153.

[176] Por. A. Adamski, *Prawo karne komputerowe...*, s. 51.

tzw. procedury autentyzacyjnej i dostaje się do systemu bez konieczności podawania hasła zabezpieczającego, a tym samym — bez potrzeby przełamywania zabezpieczeń.[177] W omawianym przypadku sprawca, co prawda, nie oddziałuje bezpośrednio na specjalne zabezpieczenia informacji, lecz dokonuje innych specjalistycznych czynności w systemie, które prowadzą do deaktywacji zabezpieczenia. Z tego też względu jego zachowanie uznać można za przełamanie zabezpieczenia, sprawca wpływa bowiem na funkcjonowanie zabezpieczenia i dzięki temu uzyskuje dostęp do informacji.[178]

Z punktu widzenia elementów charakteryzujących stronę podmiotową przestępstwa hackingu art. 267 § 1 k.k., nie wywołuje ono większych kontrowersji. Przestępstwo to ma charakter umyślny. Jak podkreśla się w piśmiennictwie, mimo braku wyraźnego ograniczenia umyślności wyłącznie do zamiaru bezpośredniego, popełnić je można w zasadzie jedynie *cum dolo directo*.[179] To ograniczenie strony podmiotowej wynika z istoty czynności wykonawczej, która wymaga świadomości sprawcy, iż uzyskuje on informację dla niego nieprzeznaczoną.[180]

NIELEGALNY PODSŁUCH I INWIGILACJA PRZY UŻYCIU ŚRODKÓW TECHNICZNYCH

Swoistym uzupełnieniem zakresu kryminalizacji wyznaczonej przez art. 267 § 1 k.k. są postanowienia przepisu art. 267 § 2 k.k., chroniącego poufność przekazu informacji. Zgodnie z brzmieniem art. 267 § 2 k.k., karze ograniczenia wolności albo pozbawienia wolności do lat 2 podlega ten, kto „w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym". Z punktu widzenia możliwych form ochrony informacji w kontekście nowoczesnych technologii cyfrowych, przepis art. 267 § 2 k.k. nakierowany jest jednoznacznie na sferę związaną z zachowaniem tajemnicy (poufności) przekazu informacji. Mniejsze znaczenie w perspektywie znamion przestępstwa „podsłuchu komputerowego" mają dwa pozostałe elementy związane z płaszczyznami ochrony informacji gromadzonych w systemach informatycznych, tj. dostępności i integralności informacji. Przez dostępność informacji rozumie się możliwość korzystania z niej przez osobę uprawnioną w każdym momencie,[181] integralność informacji rozumiana jest natomiast jako gwarancja nienaruszalności danych, zaś poufność informacji to wyłączność dostępu do niej osób uprawnionych. Wedle wytycznych OECD, przez poufność informacji rozumieć należy „właściwość danych i informacji, polegającą na ujawnianiu ich wyłącznie uprawnionym podmiotom i na potrzeby określonych procedur, w dozwolonych wypadkach i w dozwolony sposób".[182] Ochrona poufności (tajemnicy) informacji obejmuje wszelkie gwarancje wyłącznego dysponowania przez osobę uprawnioną określonym rodzajem informacji. Jak podkreśla się w literaturze, podstawową funkcją analizowanego przepisu jest ochrona sfery prywatności człowieka przed wszelkimi nieuprawnionymi formami inwigilacji, dokonywanymi przy wykorzystaniu specjalnych środków i urządzeń technicznych.[183] Z punktu widzenia pozakarnych regulacji odnoszących się do ochrony prywatności, przepis art. 267 § 2 k.k. sankcjonuje naruszenia zagwarantowanych konstytucyjnie: prawa do prywatności (art. 47 Konstytucji RP), prawa do wolności i tajemnicy komunikowania się (art. 49 Konstytucji RP) oraz prawa do nienaruszalności mieszkania (art. 50 Konstytucji RP).

Zachowanie karalne określone w znamionach przestępstwa przewidzianego w art. 267 § 2 k.k. obejmuje podejmowanie przez osoby nie posiadające prawa do określonych informacji czynności, które polegają na zakładaniu lub posługiwaniu się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym. Istota czynności karalnej sprowadza się do „podsłuchiwania", które z punktu widzenia technicznych możliwości polegać może albo na klasycznym przechwytywaniu treści informacji podczas procesu komunikowania się (podsłuchiwania przekazywanych informacji), albo na wykorzystywaniu dla uzyskiwania informacji urządzeń wizualnych bądź innych urządzeń specjalnych do uzyskiwania odpowiednich informacji. Podkreślić należy, iż możliwość uzyskania informacji zgromadzonych na komputerowych nośnikach obejmuje znacznie szerszy zakres technicznych sposobów. Obok stosowania klasycznych metod podsłuchu, przejawiających się w stosowaniu

[177] Zob. szerzej A. Adamski, *Karalność hackingu...*, s. 153–155; tenże, *Przestępstwa komputerowe...*, s. 152.

[178] Odmiennie rozstrzyga kwestię kwalifikacji hackingu przyjmującego postać *IP spoofing* A. Adamski, zdaniem którego „kwalifikacja prawna tej postaci hackingu na podstawie art. 267 § 1 k.k. może budzić wątpliwości. Sprawca nie oddziałuje bowiem bezpośrednio na istniejące zabezpieczenia i nie usuwa ich — co semantycznie odpowiadałoby pojęciu «przełamania», jakim posługuje się art. 267 § 1 k.k., lecz dokonuje obejścia zabezpieczeń, co jest czynnością wykonawczą, która nie należy do znamion omawianego przepisu" (*Prawo karne komputerowe...*, s. 51).

[179] Tak m.in. A. Marek, *Komentarz...*, s. 275.

[180] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1008; O. Górniok (w:) *Kodeks karny...*, s. 323.

[181] Pojęcie „dostępności" informacji szeroko analizuje A. Adamski, *Prawo karne komputerowe...*, s. 41.

[182] Tekst Wytycznych OECD podaję za A. Adamskim, *Prawo karne komputerowe...*, s. 42.

[183] Tak m.in. A. Adamski, *Prawo karne komputerowe...*, s. 56.

specjalnych urządzeń telekomunikacyjnych, optycznych, nokto- i termowizyjnych, elektronicznych, stosowaniu form podglądu elektronicznego, do uzyskiwania informacji bez zgody osoby będącej jej dysponentem dostępne współcześnie urządzenia techniczne umożliwiają przechwytywanie informacji przy pomocy m.in. analizy promieniowania elektromagnetycznego, emitowanego przez pracujący sprzęt komputerowy, analizy fal akustycznych emitowanych przez urządzenia komputerowe.[184] Istnieją także możliwości przejmowania informacji przesyłanych poprzez pocztę elektroniczną przy wykorzystaniu specjalnych programów komputerowych, które powodują automatyczne przesyłanie na wskazany komputer kopii wysyłanych informacji elektronicznych lub przechwytywanie informacji poprzez analizę uderzeń w klawiaturę komputera podczas wprowadzania informacji do systemu.[185] Stąd też współcześnie informacja zgromadzona na komputerowych nośnikach narażona jest na znacznie większe niebezpieczeństwo przechwycenia przez osobę nieuprawnioną.

Istotnym elementem charakteryzującym znamiona przestępstwa podsłuchu jest brak uprawnienia sprawcy do określonej informacji, na której pozyskanie nakierowane są czynności polegające na zakładaniu lub posługiwaniu się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym. Zawarta w art. 267 § 2 k.k. klauzula normatywna odnosząca się do uprawnienia do informacji określa negatywnie podmiot przestępstwa, którym może być jedynie osoba nieuprawniona do dysponowania daną informacją. Taki sposób ujęcia znamion przestępstwa z art. 267 § 2 k.k. nie zmienia niczego w odniesieniu do charakteru typu z punktu widzenia określenia podmiotu przestępstwa. Przestępstwo przewidziane w art. 267 § 2 k.k. pozostaje przestępstwem powszechnym, z tym jedynie ograniczeniem, iż jego sprawcą, z oczywistych powodów, nie może być osoba uprawniona do dysponowania informacją.[186]

[184] Zob. szerzej A. Adamski, *Prawo karne komputerowe...*, s. 58–60; K. Dudka, *Podsłuch komputerowy w polskim procesie karnym — wybrane zagadnienia praktyczne*, Prokuratura i Prawo 1999, nr 1, s. 70 i n.

[185] Opis tej techniki pozyskiwania informacji przedstawia A. Adamski, przywołując przykład specjalnych programów komputerowych stworzonych przez amerykańskich hakerów przechwytujących informacje poprzez analizę uderzeń w klawiaturę komputera. Zob. szerzej A. Adamski, *Prawo karne komputerowe...*, s. 57, zwłaszcza przyp. 4.

[186] Identyczne stanowisko zajmuje w tej kwestii W. Wróbel, stwierdzając: „Przestępstwo z art. 267 § 2 k.k. ma charakter powszechny. Nie może być jego sprawcą osoba uprawniona do uzyskania danych informacji" (*Uwagi wprowadzające...*, s. 1008). Tak samo A. Marek, wskazując na różnicę pomiędzy typem określonym w art. 267 § 2 k.k. a przestępstwem przewidzianym w art. 266 k.k., które ma charakter indywidualny (*Komentarz...*, s. 275) oraz O. Górniok (w:) *Kodeks karny...*, s. 323. W okresie obowiązywania k.k. z 1969 r. przestępstwo określone w art. 172 k.k., stanowiące częściowy odpowiednik art. 267 k.k. z 1997 r. uznawane było przez część przedstawicieli doktryny za przestępstwo indywidualne, ze względu na występujące w art. 172 k.k. znamię „bez uprawnienia". Stanowisko takie zajmował m.in. W. Świda (w:) *Kodeks karny z komentarzem...*, s. 506; O. Chybiński (w:) O. Chybiński, W. Gutekunst, W. Świda, *Prawo karne. Część szczególna*, Wrocław 1980, s. 220. Odmienne stanowisko zajmował T. Bojarski, uznając przestępstwo z art. 172 k.k. z 1969 r. za przestępstwo powszechne. Zob. szerzej T. Bojarski (w:) *System prawa karnego*, t. IV. *O przestępstwach w szczególności*, cz. II, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1989, s. 75. Por. też W. Wolter, *Klauzule normatywne w przepisach karnych*, Krakowskie Studia Prawnicze 1969, R. II, z. 3–4, s. 29 i n.

Przepis art. 267 § 2 k.k. wyraża normę sankcjonowaną, która zakazuje naruszania poufności informacji poprzez czynności polegające na zakładaniu lub posługiwaniu się urządzeniem podsłuchowym, wizualnym lub innym urządzeniem specjalnym. Wynikający z tej normy sankcjonowanej zakaz ma charakter generalny, obejmuje bowiem wszelkie czynności zmierzające do naruszenia tajemnicy informacji w sposób określony w art. 267 § 2 k.k. *Prima facie* wydawać by się mogło, że zakaz naruszania poufności informacji zawarty w art. 267 § 2 k.k. ma charakter bezwzględny, odnosi się bowiem do wszystkich podmiotów nie posiadających prawa do dysponowania informacją. W kontekście tego drugiego twierdzenia na szczególne podkreślenie zasługuje fakt, iż karnoprawna ochrona tajemnicy (poufności) informacji dotyczy nie tylko ochrony przed bezprawnymi zamachami pochodzącymi od obywateli, lecz także przed zamachami pochodzącymi od funkcjonariuszy państwowych.[187] Zarazem jednak obowiązujące przepisy prawa zawierają regulacje szczególne, które stwarzają podstawy do uzyskiwania przez określone podmioty informacji przy wykorzystaniu techniki oraz urządzeń określonych w art. 267 § 2 k.k. Istnienie tych przepisów oznacza, iż ustawodawca w niektórych, niewątpliwie wyjątkowych i szczególnych wypadkach, kierując się uzasadnionym interesem publicznym, legalizuje naruszenia poufności informacji, dokonujące się w sposób opisany jako karalny przez znamiona art. 267 § 2 k.k. W piśmiennictwie karnistycznym dominuje pogląd, iż szczególne regulacje prawne zezwalające na stosowanie przez określone organy państwowe urządzeń podsłuchowych traktowane być winny jako pozakodeksowe kontratypy, którym w dogmatyce przydaje się nazwę „działania w ramach szczególnych uprawnień i obowiązków".[188] Należy jednak podkreślić, że charakter normatywny (dyrektywalny) przepisów zezwalających na naruszenie określonych dóbr prawnych w ramach wykonywania szczególnych uprawnień i obowiązków przez funkcjonariuszy odpowiednich organów państwo-

[187] Zob. K. Dudka, *Kontrola i utrwalanie rozmów telefonicznych w projekcie kodeksu postępowania karnego z 1991 r.*, Przegląd Sądowy 1994, nr 7–8, s. 129. Por. też T. Taras, *O dopuszczalności i legalności podsłuchu telefonicznego*, Annales UMCS, Sectio G, Lublin 1960, s. 35 i n.

[188] Zob. m.in. W. Wolter, *Nauka o przestępstwie*, Warszawa 1973, s. 199; J. Śliwowski, Prawo karne, Warszawa 1979, s. 168; K. Buchała, A. Zoll, *Polskie prawo karne*, Warszawa 1995, s. 137; A. Marek, *Prawo karne...*, s. 183.

wych istotnie różni się od normatywnego zezwolenia na przekroczenie zakazu/nakazu, wyrażonego w określonych w Kodeksie karnym tzw. okolicznościach wyłączających bezprawność (kontratypach). Z tego względu uznanie przepisów zezwalających na dokonywanie przez funkcjonariuszy organów państwowych czynności stanowiących przekroczenie zakazów/nakazów w sposób zgodny z ustawową charakterystyką czynu zabronionego za pozakodeksowe kontratypy, zwłaszcza przy przyjęciu określonej koncepcji teoretycznej w odniesieniu do okoliczności wyłączających bezprawność,[189] budzić może pewne wątpliwości. Z uwagi na ramy niniejszego opracowania, zagadnienie to nie może zostać poddane w tym miejscu szczegółowej analizie;[190] pomijając teoretyczne spory związane ze statusem przepisów określających szczególne uprawnienia i obowiązki, podnieść jedynie należy, iż istnienie przepisów zezwalających na stosowanie urządzeń podsłuchowych lub innych środków technicznych umożliwiających uzyskiwanie informacji przez odpowiednie organy państwowe wpływa na zawężenie zakresu zastosowania przepisu art. 267 § 2 k.k., określając zarazem dopuszczalne (nieuznawane przez ustawodawcę za bezprawne) sposoby uzyskiwania informacji zgromadzonych w systemach komputerowych.

Podstawowym aktem prawnym, który określa zasady stosowania urządzeń podsłuchowych lub innych środków pozwalających na uzyskanie informacji jest Kodeks postępowania karnego. W art. 237 § 1 k.p.k. stanowi się, że „po wszczęciu postępowania sąd na wniosek prokuratora może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub w celu zapobieżenia popełnieniu nowego przestępstwa". Stanowiący uzupełnienie treści art. 237 k.p.k. przepis art. 241 k.p.k. stanowi, że „przepisy rozdziału niniejszego (tj. rozdziału 26 k.p.k.) stosuje się odpowiednio do kontroli oraz utrwalania przy użyciu środków technicznych treści przekazów informacji innych niż rozmowy telefoniczne". Powołane wyżej przepisy k.p.k. określają podstawy stosowania podsłuchu rozmów telefonicznych lub używania innych środków technicznych umożliwiających utrwalanie treści przekazów innych niż rozmowy telefoniczne na etapie postępowania przygotowawczego.[191] Obok regulacji zawartych w Kodeksie postępowania karnego, istnieją w polskim systemie prawnym przepisy, które pozwalają na umożliwiające stosowanie urządzeń podsłuchowych oraz innych środków technicznych umożliwiających uzyskiwanie informacji oraz utrwalanie dowodów w trakcie przeprowadzania czynności operacyjno–rozpoznawczych poza postępowaniem karnym.[192]

Wśród tej kategorii przepisów wymienić należy w szczególności art. 10 ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa, wedle którego: „Przy wykonywaniu czynności operacyjno–rozpoznawczych, w zakresie nie objętym przepisami Kodeksu postępowania karnego, podejmowanych przez Urząd Ochrony Państwa w celu realizacji zadań określonych w art. 1 ust. 2 pkt 1–5, a także w celu zapobieżenia lub wykrycia przestępstw ściganych na mocy umów i porozumień międzynarodowych, Szef Urzędu Ochrony Państwa, po uzyskaniu pisemnej zgody Prokuratora Generalnego, może zarządzić na czas określony kontrolę korespondencji, a także stosowanie środków technicznych, umożliwiających uzyskiwanie w sposób tajny informacji oraz utrwalanie dowodów. Szef Urzędu Ochrony Państwa bieżąco informuje Prokuratora Generalnego o wynikach prowadzonych czynności." Regulacja zawarta w art. 10 ust. 1 uzupełniona została poprzez postanowienia art. 10a ust. 3, zgodnie z którym w czasie wykonywania czynności określonych w art. 10a ust. 1 może być stosowana kontrola korespondencji i środki techniczne na zasadach określonych w art. 10.

Prawo do stosowania środków pozwalających na uzyskanie informacji zawarte jest także w art. 19 ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji. Wedle tego przepisu, „przy wykonywaniu czynności operacyjno–rozpoznawczych, w zakresie nie objętym przepisami Kodeksu postępowania karnego, podejmowanych przez Policję w celu zapobieżenia lub wykrycia przestępstw umyślnych (...) Minister Spraw Wewnętrznych i Administracji, po uzyskaniu

[189] Chodzi tutaj o recypowaną na grunt polski przez A. Zolla koncepcję, traktującą kontratypy jako okoliczności wtórnie legalizujące zachowanie. Zob. szerzej A. Zoll, *Okoliczności wyłączające bezprawność czynu*, Warszawa 1982, s. 101–120; tenże, *Odpowiedzialność lekarza za niepowodzenie w leczeniu*, Warszawa 1988, s. 6–16; K. Buchała, A. Zoll, *Polskie prawo karne*, Warszawa 1995, s. 196–219.

[190] W nieco szerszym aspekcie problemowi dyrektywalnego statusu tzw. szczególnych uprawnień i obowiązków postrzeganych w kontekście prawa do użycia broni palnej i środków bezpośredniego przymusu przez funkcjonariuszy Policji poświęcone są następujące opracowania: M. Dąbrowska–Kardas, P. Kardas, Glosa do postanowienia SN z 27 października 1994 r., Palestra 1996, nr 7–8, s. 276 i n.; J. Widacki, P. Kardas, J. Wójcikiewicz, *Użycie broni palnej przez Policję w Polsce w świetle standardów międzynarodowych oraz aktualnie obowiązujących przepisów* (w:) *Bezpieczny Obywatel — Bezpieczne Państwo*, red. J. Widacki, J. Czapska, Lublin 1998, s. 195–232.

[191] „Kontrola i utrwalanie rozmów telefonicznych dopuszczalne jest po wszczęciu postępowania — stwierdzają P. Hofmański, E. Sadzik, K. Zgryzek — przy czym wystarczające jest wszczęcie postępowania przygotowawczego w fazie *ad rem*" (*Kodeks postępowania karnego, Komentarz*, t. I, red. P. Hofmański, Warszawa 1999, s. 858). Zob. też R.A. Stefański (w:) J. Bratoszewski, L. Gardocki, Z. Gostyński (red.), S.M. Przyjemski, R.A. Stefański, S. Zabłocki, *Kodeks postępowania karnego. Komentarz*, t. I, Warszawa 1998, s. 601.

[192] Zdaniem A. Marka, istnienie przepisów pozwalających na stosowanie podsłuchu oraz innych środków technicznych umożliwiających uzyskiwanie informacji w sposób tajny w trakcie prowadzenia czynności operacyjno–rozpoznawczych prowadzi do poważnego uszczerbku zasady sądowej ochrony sfery prywatności i tajemnicy informacji (*Komentarz...*, s. 275).

pisemnej zgody Prokuratora Generalnego, może zarządzić, na czas określony, kontrolę korespondencji, a także stosowanie środków technicznych umożliwiających uzyskiwanie w sposób tajny informacji oraz utrwalanie dowodów. Minister Spraw Wewnętrznych i Administracji bieżąco informuje Prokuratora Generalnego o przeprowadzonych czynnościach oraz o ich wyniku."

Analogiczne uprawnienie zawarte jest w art. 36 ust. 3 ustawy z dnia 28 września 1991 r. o kontroli skarbowej. Wedle tego przepisu, „w celu wykrycia przestępstw: gospodarczych, przeciwko mieniu znacznej wartości oraz skarbowych, polegających na uszczupleniu podatku lub innej należności Skarbu Państwa znacznej wartości — Generalny Inspektor Kontroli Skarbowej, po uzyskaniu zgody Prokuratora Generalnego, może zarządzić na czas określony stosowanie środków technicznych, umożliwiających w sposób tajny uzyskiwanie informacji oraz utrwalanie śladów i dowodów".

Wreszcie podstawę do stosowania odpowiednich środków pozwalających na uzyskanie informacji przewiduje art. 15 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, w którym stanowi się, że „w zakresie zadań wykonywanych przez wojskowe służby informacyjne Ministrowi Obrony Narodowej przysługują odpowiednio uprawnienia Ministra Spraw Wewnętrznych przewidziane w ustawie o Urzędzie Ochrony Państwa i przepisach wydanych na jej podstawie".

Wszystkie wymienione wyżej przepisy zawierają regulacje, które legalizują działania podejmowane przez odpowiednie organy państwowe, polegające na utrwalaniu treści rozmów telefonicznych lub stosowaniu innych środków pozwalających na uzyskiwanie informacji w sposób tajny. Z normatywnego punktu widzenia, rozwiązania zawarte w powołanych wyżej ustawach prowadzą do ograniczenia zakresu ochrony informacji przed zamachami opisanymi w art. 267 § 2 k.k. Ich istnienie w systemie prawnym opiera się na treści art. 49 Konstytucji RP, który dopuszcza możliwość wprowadzenia regulacji ograniczającej zasadę wolności i ochrony tajemnicy komunikowania się, wskazując jednocześnie, iż takie ograniczenie nastąpić może jedynie poprzez odpowiednią regulację ustawową. Tym samym należy stwierdzić, iż poza przypadkami wyraźnie uregulowanymi w przepisach rangi ustawowej, które przyznają organom władzy publicznej uprawnienia do uzyskiwania w szczególnych wypadkach informacji przy zastosowaniu wymienionych w art. 267 § 2 k.k. sposobów, wszelkie inne sposoby uzyskiwania informacji przez osoby nie posiadające odpowiednich uprawnień stanowią naruszenie zakazu, jaki wynika z art. 267 § 2 k.k. i mogą stanowić podstawę odpowiedzialności karnej.[193]

[193] Por. A. Adamski, *Prawo karne komputerowe*..., s. 63.

Z perspektywy ochrony informacji zgromadzonych, przetwarzanych i przesyłanych przy pomocy nowoczesnych urządzeń cyfrowych, wskazać można dość istotną różnicę między zakresem uprawnień przyznanych przez przepisy k.p.k. organom procesowym a zakresem uprawnień, jakie określone zostały dla organów prowadzących czynności operacyjno–rozpoznawcze.

Artykuł 237 § 1 w zw. z art. 241 k.p.k. stwarza podstawy do przeprowadzania kontroli i utrwalania rozmów telefonicznych oraz przeprowadzania kontroli i utrwalania przy użyciu środków technicznych treści przekazów informacji innych niż rozmowy telefoniczne. Z punktu widzenia informacji zgromadzonych w systemach komputerowych, prowadzenie kontroli oraz utrwalanie treści odnosić się może jedynie do takich informacji, które w chwili stosowania odpowiednich środków technicznych podlegają procesowi wymiany (komunikacji) pomiędzy dwoma podmiotami korzystającymi z tego samego lub z połączonych systemów komputerowych. Słusznie wskazuje K. Dudka, że przepis art. 241 k.p.k. zezwala jedynie na kontrolę i utrwalanie treści przekazów informacji innych niż rozmowy telefoniczne. Oznacza to, że uzyskiwanie informacji zgromadzonych w systemie komputerowym przy wykorzystaniu znanych technik, takich jak np. analiza transmisji teleinformatycznych czy fal akustycznych emitowanych przez drukarki, nie jest objęte zakresem art. 241 k.p.k. Fale elektromagnetyczne i akustyczne nie mają bowiem charakteru treści przekazów informacji.[194]

Przepisy, które umożliwiają stosowanie środków technicznych służących do uzyskiwania informacji w sposób tajny, zawarte w ustawie o Policji, ustawie o UOP, ustawie o kontroli skarbowej oraz w ustawie o powszechnym obowiązku obrony RP, oprócz możliwości kontrolowania i utrwalania przekazów treści przechwytywanych podczas komunikowania się dwóch podmiotów w ramach systemu komputerowego, pozwalają ponadto na uzyskiwanie i utrwalanie informacji przy wykorzystaniu wszelkich innych dostępnych technik, w tym oczywiście techniki przejmowania danych za pomocą transmisji teleinformatycznych oraz analizy fal akustycznych. Przepisy te nie ograniczają możliwości stosowania środków technicznych wyłącznie do kontroli i utrwalania przekazów informacji innych niż rozmowy telefoniczne, lecz stwarzają generalną podstawę do uzyskiwania przy wykorzystaniu tych środków informacji w sposób tajny.[195]

Zachowanie karalne opisane w art. 267 § 2 k.k. polega na zakładaniu lub posługiwaniu się urządzeniem podsłuchowym, wizualnym albo innym urzą-

[194] Zob. szerzej K. Dudka, *Podsłuch komputerowy w polskim procesie karnym — wybrane zagadnienia praktyczne*, Prokuratura i Prawo 1999, nr 1, s. 70.
[195] Identycznie K. Dudka, *Podsłuch komputerowy*..., s. 70.

dzeniem specjalnym. Pojęcie zakładania obejmuje, jak podkreśla W. Wróbel, „wszelkie czynności polegające na instalowaniu urządzenia w miejscu pozyskiwania informacji".[196] Z uwagi na właściwości współczesnych urządzeń służących do zdobywania informacji w trakcie procesu komunikowania się, użyte przez W. Wróbla sformułowanie „w miejscu pozyskiwania informacji" rozumiane być winno stosunkowo szeroko. Takim miejscem może być miejsce prowadzenia procesu komunikowania się, może być to jednak miejsce znacznie oddalone od miejsca, w którym lub z którego prowadzona jest komunikacja i w jej trakcie przekazywane są informacje podlegające uzyskaniu. Posługiwanie się urządzeniem podsłuchowym, wizualnym lub innym urządzeniem specjalnym obejmuje wszelkie czynności polegające na korzystaniu z tych urządzeń w miejscu pozyskiwania informacji.[197] Oba pojęcia określające w art. 267 § 2 k.k. znamiona czynnościowe ujęte zostały stosunkowo szeroko oraz powiązane ze stadium poprzedzającym uzyskanie podlegających ochronie informacji. Przepis art. 267 § 2 k.k. kryminalizuje bowiem swoiste czynności „przygotowawcze" do uzyskania w niedozwolony sposób przekazywanej informacji.[198] Zarówno „zakładanie", jak i „posługiwanie się" urządzeniem podsłuchowym, wizualnym albo innym specjalnym urządzeniem nie musi oznaczać — i co do zasady nie oznacza — iż spełniający te czynności sprawca rzeczywiście uzyskuje informacje.[199] Podstawą odpowiedzialności karnej na podstawie art. 267 § 2 k.k. jest więc stworzenie niebezpieczeństwa dla podlegającego ochronie procesu przekazywania informacji poprzez założenie urządzenia umożliwiającego uzyskiwanie informacji lub posługiwanie się takim urządzeniem. Należy zgodzić się z A. Adamskim, iż na mocy analizowanego przepisu karalne jest nie tylko samo zakładanie lub posługiwanie się specjalnymi urządzeniami, lecz także uzyskiwanie przy ich pomocy odpowiednich informacji przez osoby nieuprawnione.[200]

Zawarte w art. 267 § 2 k.k. wyliczenie technicznych środków służących do uzyskiwania informacji ma w art. 26 § 2 k.k. charakter przykładowy. Ustawodawca wskazuje, co prawda, dwa konkretne i zdefiniowane urządze-

[196] W. Wróbel, *Uwagi wprowadzające...*, s. 1008.

[197] *Ibidem*.

[198] Trafnie podkreśla W. Wróbel, że „dla realizacji znamion czynności wykonawczej wystarczające jest wyłącznie założenie urządzenia podsłuchowego, chociażby nie doszło do jego wykorzystania ani też do uzyskania przy jego pomocy określonych informacji. Podobnie karalne jest samo posługiwanie się urządzeniem podsłuchowym, nawet jeżeli nie uzyskano jeszcze żadnej informacji" (*Uwagi wprowadzające...*, s. 1009).

[199] Tak również O. Górniok (w:) *Kodeks karny...*, s. 323.

[200] A. Adamski uzasadnia swoje twierdzenie argumentem *a minore ad maius* (*Prawo karne komputerowe...*, s. 56). Podobne stanowisko zajmuje O. Górniok (w:) *Kodeks karny...*, s. 323.

nia, tj. urządzenie podsłuchowe oraz wizualne, zarazem jednak uzupełnia katalog urządzeń sformułowaniem „innym specjalnym urządzeniem". Tym samym, zakres zastosowania normy sankcjonującej wyrażonej w art. 267 § 2 k.k. obejmuje wszelkie wypadki posługiwania się przez sprawcę urządzeniami specjalnymi służącymi do uzyskiwania informacji w trakcie procesu komunikowania się. Za urządzenia podsłuchowe uznać należy wszelkie postaci urządzeń przysposobionych do uzyskiwania informacji wyrażanych dźwiękiem. Urządzeniami wizualnymi są natomiast wszelkie urządzenia pozwalające na odbiór lub rejestrację obrazu w warunkach uniemożliwiających dokonywania tych czynności przez osoby postronne.[201] W kontekście stanowiących centralny przedmiot analizy urządzeń komputerowych, które służą do gromadzenia, przetwarzania i przesyłania informacji kluczowe znaczenie ma wymieniona w art. 267 § 2 k.k. *in fine* kategoria dopełniająca, obejmująca wszelkie inne niż podsłuchowe i wizualne urządzenia specjalne, które służą do uzyskiwania informacji zabezpieczonych przed dostępem osób postronnych. Podkreślano już w tej pracy wielokrotnie, że komunikowanie się przy pomocy sieci komputerowych stwarza niezwykle szerokie możliwości uzyskiwania dostępu do przekazywanych informacji. Z jednej strony, istnieje możliwość włączania się do przewodu telekomunikacyjnego służącego do przekazywania informacji zgromadzonych na komputerach użytkowników, z drugiej — wykorzystywać można wiele innych technik pozyskiwania informacji w trakcie przekazu, takich jak przechwytywanie danych na podstawie czynności na klawiaturze komputera wykonywanych przez nadawcę; wykorzystywanie specjalnych programów komputerowych sterujących odpowiedniej klasy komputerami, umożliwiających „przechwytywanie początkowych sekwencji bajtów każdej sesji, zawierających identyfikatory i hasła użytkowników", które następnie otwierają dostęp do określonych informacji; przejmowanie i analiza transmisji elektromagnetycznych lub akustycznych. Niezwykła różnorodność i mnogość technik umożliwiających uzyskanie informacji w trakcie przekazu dokonywanego poprzez sieci komputerowe rodzić może pewne komplikacje w związku z charakterystyką znamion przestępstwa przewidzianego w art. 267 § 2 k.k. Przepis ten wymaga bowiem dla karalności posłużenia się przez sprawcę innym specjalnym urządzeniem. Zakładanie lub posługiwanie się czymś, co nie posiada statusu specjalnego urządzenia, wyklucza możliwość przypisania danej osobie wypełnienia znamion przestępstwa z art. 267 § 2 k.k. Odnosząc się do kwestii związanych z zakresem uprawnień posiadanych przez ograny procesowe oraz organy wykonujące

[201] Zob. szerzej W. Wróbel, *Uwagi wprowadzające...*, s. 1009.

czynności operacyjno–rozpoznawcze w sferze uzyskiwania w sposób tajny informacji przy wykorzystaniu specjalnych technik wskazano już, iż dla uzyskania informacji poprzez analizę fal elektromagnetycznych oraz fal akustycznych konieczne jest posługiwanie się specjalnymi urządzeniami. Stąd też, niewątpliwie, stosowanie tej techniki poza przypadkami wymienionymi w przepisach szczególnych stanowi naruszenie zakazu wynikającego z art. 267 § 2 k.k. i realizację znamion określonego w tym przepisie typu czynu zabronionego. Wątpliwości związane są natomiast z innymi, wymienionymi wyżej typowymi „komputerowymi" technikami uzyskiwania informacji. Metoda polegająca na uzyskiwaniu danych poprzez analizę czynności dokonywanych przez nadawcę na klawiaturze komputera oraz metoda polegająca na wykorzystywaniu specjalnych programów komputerowych sterujących odpowiedniej klasy komputerami, umożliwiających „przechwytywanie początkowych sekwencji bajtów każdej sesji, zawierających identyfikatory i hasła użytkowników", które następnie otwierają dostęp do określonych informacji (*password sniffer*) — w istocie sprowadzają się do wykorzystywania specjalnego oprogramowania komputerowego. W piśmiennictwie karnistycznym pojawiały się wątpliwości związane z normatywnym statusem programu komputerowego oraz komputera, który sterowany jest przez ten program, w kontekście znamienia „inne specjalne urządzenie". Z jednej strony, w literaturze nie wywołuje kontrowersji twierdzenie, że sam program komputerowy nie może zostać uznany za desygnat pojęcia „urządzenie", którym posługuje się przepis art. 267 § 2 k.k.[202] Zarazem jednak istnieje zasadnicza rozbieżność co do kwalifikacji komputera wyposażonego w taki specjalny program komputerowy. Zdaniem części autorów, „nie mają charakteru urządzenia specjalnego wszelkie takie urządzenia służące do uzyskiwania informacji, które mają charakter urządzeń powszechnie dostępnych, nawet jeżeli sposób lub okoliczności ich użycia noszą znamiona naruszenia dóbr osobistych osoby, której dotyczą informacje", co w konsekwencji prowadzi do wniosku, iż „program komputerowy nie może być traktowany jako urządzenie specjalne. Nie można traktować także za takie urządzenie komputera, na którym zainstalowano wyżej opisane oprogramowanie".[203] Wedle ujęcia alternatywnego, mimo iż sam program komputerowy nie może zostać uznany za urządzenie specjalne, to zainstalowany na odpowiednim komputerze, staje się łącznie z komputerem urządzeniem specjalnym w rozumieniu art. 267 § 2 k.k. Zwolennicy tego ujęcia wskazują,

[202] Tak m.in. A. Adamski, *Prawo karne komputerowe...*, s. 58; W. Wróbel, *Uwagi wprowadzające...*, s. 1010.
[203] W. Wróbel, *Uwagi wprowadzające...*, s. 1010.

iż w zależności od oprogramowania komputer może być wykorzystywany do bardzo różnych celów. Zainstalowanie w komputerze odpowiedniego oprogramowania, służącego do uzyskiwania informacji przekazywanych w obszarze sieci komputerowej, przekształca urządzenie powszechnie dostępne w urządzenie posiadające specjalne właściwości.[204] Odnosząc się do istniejącej w piśmiennictwie kontrowersji, za w pełni przekonywający uznać wypada pogląd, wedle którego za urządzenie specjalne nie sposób uznać urządzenia powszechnie dostępnego. Zarazem jednak nie sposób zapoznać faktu, iż sam komputer, który jest oczywiście urządzeniem powszechnie dostępnym, uzyskuje odpowiednie właściwości — określające m.in. zakres jego zastosowania — dopiero po zainstalowaniu w nim odpowiedniego oprogramowania. To właśnie w zależności od oprogramowania komputery wykorzystywane mogą być do różnorodnych celów (np. wprowadzenie do komputera programu Page Maker przekształca komputer w profesjonalną maszynę drukarską). Stąd też nie sposób mówić o komputerze jako o samym urządzeniu, konieczne jest bowiem zbadanie, w oparciu o jakie oprogramowanie ten komputer funkcjonuje. Jeśliby przyjąć ten sposób rozumowania jako uzasadniony, wówczas stwierdzić wypadnie, iż wprowadzenie do komputera specjalnego oprogramowania, umożliwiającego uzyskiwanie przez osobę nieupoważnioną informacji przekazywanych w sieci komputerowej, czyni tak „uzbrojony" komputer specjalnym urządzeniem służącym do uzyskiwania informacji. Oznaczałoby to, że obie wymienione wyżej specjalne techniki, polegające na uzyskiwaniu informacji poprzez analizę uderzeń w klawiaturę komputera lub poprzez analizę identyfikatorów i haseł użytkowników, mogłyby zostać uznane za zakładanie lub posługiwanie się specjalnym urządzeniem w rozumieniu art. 267 § 2 k.k.[205]

Z punktu widzenia strony podmiotowej, przepis art. 267 § 2 k.k. nie wywołuje większych wątpliwości. Określone w tym przepisie przestępstwo ma charakter umyślny, a z uwagi na jego kierunkowy charakter umyślność możliwa jest wyłącznie w formie zamiaru bezpośredniego. Należy podkreślić, że dla realizacji znamion strony podmiotowej konieczne jest, aby sprawca działał w celu uzyskania informacji, do których nie jest uprawniony.[206]

Artykuł 267 § 3 k.k. kryminalizuje ujawnienie informacji uzyskanej w sposób określony w art. 267 § 1 lub 2 innej osobie. Z punktu widzenia przedmiotu ochrony — którym są informacje podlegające ochronie na mocy art. 267 § 1

[204] Por. A. Adamski, *Prawo karne komputerowe...*, s. 58–59.
[205] Identycznie A. Adamski, *Prawo karne komputerowe...*, s. 59.
[206] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1010.

lub 2 k.k. — przepis art. 267 § 3 k.k. stanowi uzupełnienie zakresu ochrony. Obejmuje wszelkie zachowania polegające na ujawnieniu innej osobie informacji uzyskanych w sposób przestępny. Znamiona art. 267 § 3 k.k. nie wymagają, aby osoba ujawniające te informacje uprzednio samodzielnie uzyskała je w sposób określony w art. 267 § 1 lub 2. Sprawcą przestępstwa z art. 267 § 3 k.k. może być zarówno ten, kto uzyskał informacje w sposób określony w art. 267 § 1 lub 2, jak i osoba, która ujawnia informacje uzyskane do innej osoby. Podkreślić należy, iż w odniesieniu do tego ostatniego przypadku nie jest wymagane, aby ujawniający uzyskał informacje podlegające ujawnieniu bezpośrednio do osoby, która je w bezprawny sposób uzyskała.[207] Samo ujawnienie następować może nie tylko poprzez przekazanie informacji konkretnej osobie, lecz także poprzez opublikowanie ich lub podanie do wiadomości przy pomocy środków masowego komunikowania.

NARUSZENIE INTEGRALNOŚCI INFORMACJI — ART. 268 K.K.

12. Kolejnym nowym typem przestępstw wprowadzonych do polskiego systemu prawnego przez k.k. z 1997 r. jest przestępstwo naruszenia integralności zapisu informacji określone w art. 268 k.k. Wedle tego przepisu, kryminalizacji podlega zachowanie polegające na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu przez osobę nieuprawnioną zapisu istotnej informacji albo w inny sposób udaremnianiu lub znacznym utrudnianiu osobie uprawnionej zapoznanie się z tą informacją (art. 268 § 1 k.k.). Dopuszczenie się tych czynności w stosunku do zapisu na komputerowym nośniku informacji stanowi typ kwalifikowany przestępstwa naruszenia integralności informacji, określony w art. 268 § 2 k.k. Właśnie to przestępstwo stanowić będzie podstawowy przedmiot rozważań prowadzonych w niniejszej części opracowania, z tym jednak, iż z uwagi na charakterystyczne dla typu zmodyfikowanego związki art. 268 § 2 k.k. z opisem typu podstawowego zawartym w art. 268 § 1 k.k. w pewnym zakresie konieczne będzie także przedstawienie kilku uwag odnoszących się do tego typu. Przytoczony wyżej przepis nowego polskiego Kodeksu karnego ma swój odpowiednik w niemieckiej ustawie karnej. Zamieszczony w rozdziale XXVII StGB § 303a w ust. 1 stanowi: „Kto bezprawnie informacje (§ 202a ust. 2) usuwa, zataja, czyni niezdatnym do użytku lub zmienia, podlega karze pozbawienia wolności do lat dwóch lub grzywnie".

[207] Zob. szerzej W. Wróbel, *Uwagi wprowadzające...*, s. 1010.

Zgodnie z ust. 2 tego przepisu, „Usiłowanie jest karalne".[208] ustawowy kształt znamion przestępstwa określonego w art. 268 § 2 k.k. oraz w § 303a StGB wykazuje daleko idące podobieństwa. W obu przepisach ochronie podlegają informacje zapisane na elektronicznym nośniku danych, na który wprost wskazuje brzmienie art. 268 § 2 k.k., pośrednio zaś treść § 303a, odsyłającego w zakresie definicji informacji podlegających ochronie do § 202a ust. 2, wedle którego informacje stanowiące przedmiot przestępstwa to jedynie informacje zapisane lub przesyłane elektronicznie, magnetycznie lub w inny sposób uniemożliwiający bezpośrednie zapoznanie się z nimi.[209] Polski przepis jest nieco bardziej rozbudowany niż jego niemiecki odpowiednik, zawiera bowiem szersze wyliczenie czynności sprawczych. Ponadto polski przepis obejmuje nieznany niemieckiemu kodeksowi karnemu typ kwalifikowany, w którym okolicznością kwalifikującą jest wyrządzenie przez czyn sprawcy znacznej szkody majątkowej. Podkreślić należy, że oba przepisu zamieszczone są w innych rozdziałach Kodeksu karnego: art. 268 polskiego k.k. znajduje się w rozdziale grupującym przestępstwa przeciwko ochronie informacji, § 303a niemieckiego kodeksu karnego — w rozdziale zawierającym przestępstwa uszkodzenia rzeczy.[210]

Przepis art. 268 k.k. chroni prawo do dysponowania informacją w aspekcie prawa do zachowania integralności informacji oraz prawa dostępu do informacji.[211] Można zatem stwierdzić, że dobrem prawnie chronionym na podstawie art. 268 jest informacja. Przepis art. 268, przydając ochronę informacji, zawiera jednak szczególne ograniczenie zakresu kryminalizacji. Zgodnie z jego brzmieniem, karalne jest nie jakiekolwiek niszczenie, usuwanie, uszkadzanie lub zmienianie zapisu informacji, lecz jedynie dopuszczenie się tych czynności w stosunku do zapisu zawierającego „istotną" informację.[212]

[208] W oryginalnej wersji językowej przepis ten stanowi: § 303a. (1). *Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchtbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.* (2) *Der Versuch ist strafbar."*

[209] Zgodnie z brzmieniem przepisu § 202a Abs. 2 StGB: *„Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden".*

[210] § 303a znajduje się w „Siebenundzwanzigster Abschnitt. Sachbeschädigung".

[211] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1015. Podobnie na gruncie § 303a StGB — zob. W. Stree (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1952; F. Haft, *Das Zweite Gesetz...*, s. 10.

[212] Analogicznego ograniczenia nie zawiera przepis § 303a StGB. Należy jednak podkreślić, że w piśmiennictwie niemieckim wyraźnie wskazuje się na konieczność ograniczenia kręgu informacji podlegających ochronie na podstawie § 303a StGB jedynie do takich informacji, które stanowią bezpośrednie odzwierciedlenie określonych interesów majątkowych. W. Stree podkreśla, że *„Dementsprechend ist der Tatbestand auf Daten zu beschränken, an denen und deren Unversehrtheit ein anderer ein unmittelbares Interesse besitz"* (w: Schönke/Schröder. *Strafgesetzbuch. Kommentar...*, s. 1952).

Określenie informacji jako „istotnej" dalekie jest od wymogu jurydycznej precyzji. Mając na względzie charakter określenia „istotna" w kontekście struktury przestępstwa stwierdzić należy, iż o istotności informacji jako jednej z przesłanek odpowiedzialności karnej decydować powinny kryteria obiektywne. Zasadniczym elementem przesądzającym o istotności informacji będzie jej obiektywnie oceniane znaczenie dla podmiotu, którego informacja dotyczy. O istotności informacji decydować będą zatem przede wszystkim jej treść, waga, znaczenie. Podstawą oceny istotności jest w tym kontekście standard obowiązujący w danej dziedzinie, do której odnosi się informacja.[213] Wydaje się jednak, iż sam obiektywny wymiar informacji nie w każdym przypadku przesądzać będzie o jej kwalifikacji z punktu widzenia znamion przestępstwa z art. 268 k.k. W pewnych wypadkach obiektywny osąd wartości informacji uzupełniać należy elementami subiektywizującymi, w tym zwłaszcza interesami osoby uprawnionej do zapoznania się z informacją.[214] W literaturze prezentowany jest pogląd, iż obok obiektywnej metody wyznaczania istotności informacji, odnoszonej do jej wagi, istnieje możliwość wyznaczania istotności w odniesieniu nie tyle do samej informacji, co raczej do nakładu środków, jakie ponieść musiał pokrzywdzony dla uzyskania lub stworzenia informacji.[215] W pewnych sytuacjach — zaznaczymy od razu, że jednoznacznie wyjątkowych — o istotności informacji przesądzać można byłoby, wedle tego ujęcia, nie w oparciu o kryteria jakościowe związane z treścią informacji, lecz na podstawie kryteriów ilościowych, odwołujących się do wielkości środków koniecznych dla jej uzyskania lub stworzenia. Ten sposób interpretacji art. 268 k.k., mimo iż dobrze koresponduje z fenomenologią tej odmiany przestępstwa komputerowego[216] oraz z Dyrektywami Unii Europejskiej dotyczącymi prawnej ochrony baz danych,[217] rodzi jednak poważne wątpliwości natury dogmatycznej. Postrzegając to zagadnienie z dogmatycznego punktu widzenia wydaje się, iż kształt znamion przestępstwa z art. 268 uniemożliwia stosowanie tej metody oceny istotności informacji.[218]

[213] Tak również E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 205.

[214] Stanowisko takie zajmuje O. Górniok, stwierdzając, że „rozpoznanie ocennego określenia tej informacji jako istotnej wymaga uwzględnienia jej znaczenia dla dysponenta zapisu oraz celu, do jakiego ma ta informacja służyła" (w: *Kodeks karny...*, s. 325). Podobnie W. Wróbel, *Uwagi wprowadzające...*, s. 1019.

[215] Pogląd taki prezentuje m.in. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 205.

[216] Szeroki katalog przejawów niszczenia, uszkadzania, usuwania i zmieniania zapisów na komputerowym nośniku informacji przedstawia A. Adamski, wskazując na specyficzne metody destrukcji softwarowej, takie jak wirusy, robaki, bomby czasowe i bomby logiczne (*Przestępstwa komputerowe...*, s. 37). Tego rodzaju sposoby uszkadzania lub niszczenia informacji w pewnych przypadkach wymagają raczej oceny istotności dokonywanej w aspekcie ilościowym, nie zaś jakościowym.

[217] Zob. szerzej w tej kwestii E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 205.

Przedmiotem czynności wykonawczej przestępstwa z art. 268 § 2 k.k. jest zapis informacji. W analizowanym typie kwalifikowanym, określonym w art. 268 § 2 k.k., ustawodawca wymaga, aby zapis informacji stanowiący przedmiot czynności wykonawczej znajdował się na komputerowym nośniku informacji. Kodeks karny posługując się pojęciem „komputerowy nośnik informacji" w żaden sposób nie wyjaśnia tego terminu. Pewne komplikacje z ustaleniem jego znaczenia związane są z faktem posłużenia się przez ustawodawcę w kilku innych aktach prawnych pojęciami zbliżonymi, lecz nie równoznacznymi z pojęciem „komputerowy nośnik informacji". Tak na przykład w ustawie o rachunkowości[219] występuje termin „komputerowy nośnik danych", zaś w ustawie — Prawo bankowe[220] pojawia się pojęcie „elektroniczny nośnik informacji". Pomijając pewne zamieszanie w systemie prawnym, wynikające z posługiwania się przez ustawodawcę różnymi terminami na określenie zbliżonego przedmiotu, na którym znajdują się zapisy informacji podlegającej ochronie, należy przyjąć maksymalnie szeroką i pozbawioną technicznych naleciałości definicję „komputerowego nośnika informacji", uznając za taki wszystkie aktualnie dostępne nośniki, na których „informacja może zostać zapisana przy użyciu w tym celu komputera".[221]

Czynność wykonawcza przybierać może postać niszczenia, uszkadzania, usuwania lub zmieniania zapisu istotnej informacji albo udaremniania w inny sposób lub znacznego utrudniania osobie uprawnionej zapoznania się z tą informacją. Pierwsze cztery odmiany czynności wykonawczej charakteryzują się zamachem na integralność zapisu.[222] Niszczenie zapisu informacji polegać może albo na unicestwieniu nośnika, na którym znajduje się zapis, albo na unicestwieniu samego zapisu.[223] Uszkodzenie zapisu to wywołanie takiego

[218] Zob. uwagi na temat kwantyfikacji informacji w kontekście znamion przestępstwa z § 303a StGB — W. Stree (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1952.

[219] Zob. art. 3 ust. 1 pkt 3 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. Nr 121, poz. 591 ze zm.).

[220] Zob. art. 7, 63 i 65 ustawy z dnia 29 sierpnia 1997 r. — Prawo bankowe (Dz.U. Nr 140, poz. 939 ze zm.).

[221] Identyczną formułę wyjaśniającą pojęcie „komputerowy nośnik informacji" przyjmuje E. Czarny–Drożdżejko (*Ochrona informacji...*, s. 207). Zob. też w tej kwestii A. Adamski, *Przestępstwa komputerowe...*, s. 69–71.

[222] Por. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 206.

[223] Identycznie znamię to interpretowane jest na gruncie § 303a StGB. W. Stree stwierdza, że *„gelöscht werden Daten, wenn sie vollständig und unwiederbringlich unkenntlich gemacht werden (...) also für immer gänzlich verloren sind"* (w: Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1952). Zob. też identyczną tezę Samsona (w:) *Systematischer Kommentar...*, s. 20.

stanu rzeczy, w którym zapis nie posiada właściwości, jakimi charakteryzował się przed atakiem, co utrudnia odczytanie lub zrozumienie informacji. Uszkodzenie zapisu może wiązać się — identycznie jak zniszczenie — z działaniami nakierowanymi albo na nośnik, albo na sam zapis. Różnica między zniszczeniem a uszkodzeniem sprowadza się natomiast do tego, iż w przypadku uszkodzenia informacja pozostaje, nie ulega całkowitej likwidacji, z tym jednak, że naruszona zostaje jej integralność wpływająca na sensowność zapisu.[224] Zmiana zapisu przybierać może formę uszkodzenia lub modyfikacji zapisu rzutującej na treść zakodowanej w nim informacji. Zmiana prowadzić może albo do całkowitego pozbawienia sensu określonego zapisu, albo też do wypaczenia pierwotnego sensu w ten sposób, że informacja zawarta w zapisie pozostaje czytelna, wyraża jednak całkowicie inne treści od tych, które zakodowane były w zapisie przed zmianą. Jak podkreśla W. Wróbel, zmianą zapisu może być także zakodowanie informacji o niezmienionej treści w nowy sposób (np. w innym kodzie, innym języku itp.).[225] Dwie pozostałe postaci czynności wykonawczej, tj. udaremnianie lub znaczne utrudnianie zapoznania się z informacją, mają charakter dopełniający i nie muszą odnosić się ani do samego zapisu, ani do nośnika, na którym znajduje się zapis informacji. Spektrum możliwych odmian czynności wykonawczej jest niezwykle szerokie i obejmuje m.in. zachowania polegające na schowaniu komputera, wprowadzeniu szczególnych utrudnień dostępu do nośnika itp. Podkreślić należy, że ustawodawca ujął bardzo szeroko opis czynności wykonawczych charakteryzujących przestępstwo z art. 268 § 2 k.k., tak iż właściwie każde zachowanie naruszające integralność informacji może być zakwalifikowane na podstawie tego przepisu. Fakt ten jest jednoznacznie pozytywnie oceniany w literaturze przedmiotu.[226]

Przestępstwo określone w art. 268 § 2 k.k. może popełnić tylko osoba, która nie ma uprawnienia do uzyskania informacji.[227] Użyte przez ustawodawcę w znamionach typu sformułowanie określające podmiot przestępstwa „kto bez uprawnienia…" stworzyło podstawę do pewnej kontrowersji w piśmiennictwie. Zaprezentowano bowiem pogląd, że przestępstwo określone w art. 268 k.k. zostało skonstruowane jako przestępstwo indywidualne właściwe, „gdyż jego popełnienie w typie podstawowym zależy od posiadania przez sprawcę określonych kwalifikacji".[228] Autorka tego poglądu podkreśla, że znamię „nie będąc do tego uprawnionym" nie może zostać uznane za normatywną klauzulę, lecz stanowi element dookreślający podmiot czynu zabronionego.[229] Rozumowanie to trudno zaakceptować. Odnosząc do znamion przestępstwa z art. 268 k.k. klasyczne formuły analizy dogmatycznej można spostrzec, że formuła opisująca podmiot czynu zabronionego nie wymaga od sprawcy przestępstwa żadnych szczególnych właściwości, które wyróżniałyby go spośród innych osób i od których spełnienia uzależniona byłaby jego odpowiedzialność karna.[230] Sprawcą przestępstwa określonego w art. 268 niewątpliwie nie jest *intraneus*, lecz każdy podmiot. Jest to zatem przestępstwo powszechne.[231]

Przestępstwo naruszenia integralności informacji nie budzi większych wątpliwości z punktu widzenia ustawowego opisu strony podmiotowej. Ma ono charakter umyślny, a realizacja znamion możliwa jest zarówno z zamiarem bezpośrednim, jak i z zamiarem wynikowym.[232]

W przepisie art. 268 § 3 k.k. określone zostały znamiona typu kwalifikującego ze względu na wielkość wyrządzonej poprzez zachowanie sprawcy szkody majątkowej. Typ kwalifikowany przewidziany w tym przepisie ma specyficzną konstrukcję, albowiem normatywnym punktem odniesienia czyni zarówno typ podstawowy przewidziany w art. 268 § 1, jak i typ kwalifikowany ze względu na nośnik informacji, na który skierowane są czynności sprawcy. Obie odmiany przestępstwa, przewidziane w art. 268 § 1 i art. 268 § 2 k.k., uzyskują identyczny status z punktu widzenia zawartości bezprawia w sytuacji, jeżeli konsekwencją działania sprawcy jest wyrządzenie znacznej szkody majątkowej. Stylizacja przepisu art. 268 § 3 k.k., zwłaszcza zaś ujęcie znamienia kwalifikującego przyjmujące postać sformułowania „wyrządza znaczną szkodę majątkową", istotnie odbiega od metody stosowanej w przypadku

[224] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1016–1017.

[225] *Ibidem*, s. 1017. Por. też W. Stree (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1952.

[226] Zob. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 206.

[227] Podobny warunek przyjmuje się w piśmiennictwie niemieckim w odniesieniu do przestępstwa z § 303a StGB, chociaż sama treść tego przepisu nie zawiera ograniczenia ochrony informacji tylko do wypadków oddziaływania na zapis przez osobę nie posiadającą uprawnienia do korzystania z informacji. Ograniczenie zakresu ochrony przewidzianej w § 303a StGB wyprowadza się w literaturze niemieckiej z zestawienia tego przepisu z § 303 StGB, określającym znamiona przestępstwa zniszczenia cudzej rzeczy (*Sachbeschädigung*). Według § 303 StGB: *„Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft"*. Zob. też W. Stree (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1952.

[228] E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 206.

[229] *Ibidem*, s. 206.

[230] Zob. A. Marek, *Prawo karne...*, s. 100.

[231] Identycznie W. Wróbel, *Uwagi wprowadzające...*, s. 1016; O. Górniok (w:) *Kodeks karny...*, s. 324; J. Wojciechowski, *Kodeks karny...*, s. 470; A. Adamski, *Przestępstwa komputerowe...*, s. 68 i n.

[232] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1020; A. Adamski, *Przestępstwa komputerowe...*, s. 75 i n.; O. Górniok (w:) *Kodeks karny...*, s. 325.

konstruowania znamion typów o mieszanej stronie podmiotowej, w tym zwłaszcza tzw. przestępstw kwalifikowanych przez nieumyślne następstwo. W wypadku gdy skutek stanowiący następstwo wywołany być może nieumyślnie, wedle reguł przewidzianych w art. 9 § 3 k.k., ustawodawca określa ten skutek albo poprzez wyraźne zamieszczenie w odniesieniu do niego klauzuli nieumyślności, albo poprzez posłużenie się zwrotem „następstwo" (np. art. 156 § 3 k.k.; art. 173 § 3 k.k.). Posłużenie się zwrotem „następstwo" bez zaznaczania w opisie typu, iż ma do niego zastosowanie klauzula nieumyślności, wskazuje jednoznacznie na przepis art. 9 § 3 k.k., określający generalne zasady odpowiedzialności za typy kwalifikowane przez następstwo, wprowadzając zasadę nieumyślności następstwa. Konstrukcja zastosowana przez ustawodawcę przy opisie znamion przestępstwa z art. 268 § 3 k.k. wyraźnie wskazuje, że szkoda, stanowiąca rezultat działania sprawcy, bynajmniej nie ma charakteru następstwa w rozumieniu art. 9 § 3 k.k.[233] Tym samym, aby istniała prawnokarnie relewantna możliwość objęcia jej jedynie nieumyślnością przez sprawcę, w przepisie art. 268 § 3 k.k. musiałaby być zawarta klauzula nieumyślności odniesiona do szkody. Brak takiej klauzuli w połączeniu z niemożnością zastosowania do art. 268 § 3 k.k. reguł opisanych w art. 9 § 3 k.k. sprawia, iż także wyrządzona szkoda, aby stanowić mogła podstawę przypisania sprawcy typu kwalifikowanego, musi być objęta umyślnością co najmniej w formie zamiaru wynikowego. W zakończeniu podkreślić należy, że pojęcie znacznej szkody zostało zdefiniowane w art. 115 § 7 w zw. z § 5 i 6 k.k. Samą zaś szkodę konstytuują zarówno powstałe w wyniku popełnienia przestępstwa rzeczywiste uszczerbki w majątku pokrzywdzonego (*damnum emergens*), jak i utracone a spodziewane korzyści, których pokrzywdzony nie był w stanie osiągnąć ze względu na popełnienie przestępstwa (*lucrum cessans*).[234]

[233] Za możliwością stosowania reguły z art. 9 § 3 k.k. do przestępstwa określonego w art. 268 § 3 k.k. opowiada się O. Górniok, stwierdzając, że „przepis § 3 przewiduje typ kwalifikowany ze względu na następstwo, którym jest znaczna szkoda majątkowa. Zgodnie z art. 9 § 3, może ono być objęte nieumyślnością" (w: *Kodeks karny*..., s. 325).

[234] Zob. szerzej w tej kwestii P. Kardas (w:) K. Buchała, P. Kardas, J. Majewski, W. Wróbel, *Komentarz do ustawy o ochronie obrotu gospodarczego*, Warszawa 1995, s. 23–25; P. Kardas, *Szkoda majątkowa jako znamię przestępstwa nadużycia zaufania*, Prokuratura i Prawo 1996, nr 7–8, s. 36 i n.; J. Skorupka, *Szkoda majątkowa jako znamię przestępstwa z art. 9 ustawy o ochronie obrotu gospodarczego*, Prokuratura i Prawo 1997, nr 9, s. 69–75; A. Adamski, *Przestępstwa komputerowe*..., s. 77–78.

SABOTAŻ KOMPUTEROWY — ART. 269 K.K.

13. Trzecią odmianą przestępstwa związanego z komputerowymi nośnikami informacji, nie znaną Kodeksowi karnemu z 1969 r., jest określony w art. 269 k.k. z 1997 r. sabotaż komputerowy. Zgodnie z brzmieniem § 1 tego przepisu: „Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8". Wedle § 2 art. 269 natomiast: „Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji". Przepis ten pozostaje w ścisłym związku z procesem ujednolicania ustawodawstwa karnego w Europie, albowiem sabotaż komputerowy należy do kategorii przestępstw objętych tzw. listą minimalną w Zaleceniach Komitetu Ministrów Rady Europy.[235] Na razie tylko część z europejskich ustawodawstw karnych zawiera przepisy kryminalizujące sabotaż komputerowy,[236] w tym też sensie rozwiązanie przyjęte w nowym Kodeksie karnym uznać należy za krok w bardzo dobrym kierunku. Odpowiednik art. 269 k.k. znajduje się w niemieckim kodeksie karnym, którego § 303b ust. 1 stanowi: „Kto przetwarzanie informacji mających istotne znaczenie dla obcego przedsiębiorstwa, zakładu lub organu zakłóca przez to, że: 1. popełnia czyn określony w § 303a lub 2. urządzenie służące do przetwarzania danych lub urządzenie, na którym dane są zapisane uszkadza, czyni niezdatnym do użytku, usuwa lub zmienia, podlega karze pozbawienia wolności do lat pięciu lub grzywnie". Wedle ust. 2: „Usiłowanie jest karalne".[237]

[235] Zob. szerzej A. Adamski, *Przestępstwa komputerowe w projekcie kodeksu karnego na tle europejskich standardów normatywnych* (w:) *Przestępczość komputerowa*, red. A. Adamski, Poznań 1994, s. 141–159; tenże, *Przestępstwa komputerowe*..., s. 79 i n.; E. Czarny–Drożdżejko, *Ochrona informacji*..., s. 207.

[236] A. Adamski podaje, że w Europie zachodniej karalność sabotażu komputerowego przewiduje jedynie ustawodawstwo Danii, Finlandii, Holandii i Niemiec (*Przestępstwa komputerowe*..., s. 79, przyp. 110).

[237] W oryginalnym brzmieniu przepis ten stanowi: § 303b *Computersabotage* (1) *Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er 1. eine Tat nach § 303a Abs. 1 begeht oder 2. eine Datenverarbeitungsanlage oder Datenträger zarstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.* (2) *Der Versuch ist strafbar.*

Przepis art. 269 k.k. odbiega nieco od pozostałych typów przestępstw zgromadzonych w rozdziale XXXIII k.k. Istotna odmienność sprowadza się do określenia przedmiotu ochrony. Głównym przedmiotem ochrony czynu zabronionego określonego w art. 269 k.k. jest bowiem specyficzny rodzaj informacji, mającej szczególne znaczenie dla obronności, komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej.[238] Przyglądając się ustawowej charakterystyce informacji podlegającej ochronie na mocy analizowanego przepisu można zauważyć, iż na jego podstawie kryminalizowane są zachowania godzące bezpośrednio w szczególny rodzaj informacji, pośrednio zaś w podstawy obronności, bezpieczeństwo w komunikacji oraz funkcjonowanie administracji rządowej i samorządowej.[239] Z tego punktu widzenia przepis art. 269 k.k. wykazuje pewne podobieństwo w zakresie funkcji kryminalizacyjnej[240] do przestępstw określonych w rozdziale XVIII k.k. pt. „Przestępstwa przeciwko obronności", przestępstw zgrupowanych w rozdziale XXI pt. „Przestępstwa przeciwko bezpieczeństwu w komunikacji", przestępstw z rozdziału XXIX pt. „Przestępstwa przeciwko działalności instytucji państwowych oraz samorządu terytorialnego" oraz w rozdziale XX pt. „Przestępstwa przeciwko bezpieczeństwu powszechnemu".[241] Przestępstwo opisane w art. 269 k.k. ma charakter abstrakcyjnego narażenia na niebezpieczeństwo. W każdym wypadku, gdy sabotaż komputerowy doprowadzi do powstania konkretnego niebezpieczeństwa dla określonych dóbr lub powstania szkody w jednej z dziedzin, które wyznaczają w znamionach tego typu zakres informacji o szczególnym znaczeniu, kwalifikacja zachowania sprawcy opierać się będzie na odpowiednim przestępstwie konkretnego narażenia na niebezpieczeństwo lub przestępstwie skutkowym zawartym we właściwym rozdziale Kodeksu karnego. Jedynie tytułem przykładu można w tym miejscu wskazać, że wywołanie w wyniku sabotażu komputerowego zagrożenia dla życia lub zdrowia wielu osób lub mienia w wielkich rozmiarach przez zachowanie sprawcy spełniające warunki czynności wykonawczej określone w art. 269 § 1 k.k. (a więc poprzez

[238] Por. A. Adamski, *Przestępstwa komputerowe...*, s. 80; E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 207 i n.; O. Górniok (w:) *Kodeks karny...*, s. 326; W. Wróbel, *Uwagi wprowadzające...*, s. 1023.

[239] Analogicznie jest w przypadku przestępstwa określonego w § 303b StGB, który chroni informacje mające istotne znaczenie dla gospodarki lub administracji — zob. szerzej W. Stree (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1954.

[240] Co do zagadnień związanych z teoriami i funkcjami kryminalizacji — zob. szerzej L. Gardocki, *Zagadnienia teorii kryminalizacji*, Warszawa 1990, passim.

[241] Zob. O. Górniok (w:) *Kodeks karny...*, s. 326; A. Adamski, *Przestępstwa komputerowe...*, s. 83.

sabotaż komputerowy) kwalifikowane będzie na podstawie art. 165 § 1 k.k.,[242] zaś wywołanie w wyniku usunięcia z komputera wojskowego informacji służących do sterowania określonego rodzaju bronią specjalistyczną — w wyniku czego dojdzie do zniszczenia lub uszkodzenia obiektu o znaczeniu obronnym — podlegać będzie kwalifikacji na podstawie art. 140 § 1 k.k.[243]

Informacja stanowiąca przedmiot ochrony czynu zabronionego z art. 269 k.k. musi z obiektywnego punktu widzenia mieć szczególne znaczenie dla jednej z dziedzin wymienionych w tym przepisie.[244] W tym przypadku nie istnieją możliwości subiektywizacji oceny znaczenia informacji jako przedmiotu ochrony.[245]

Elementem charakteryzującym czyn zabroniony określony w art. 269 k.k. jest, obok charakteru informacji, także nośnik, na którym jest ona zapisana. Znamiona sabotażu komputerowego ograniczają zakres kryminalizacji tylko do informacji, których zapis znajduje się na komputerowym nośniku informacji. Określenie nośnika jest w omawianym przepisie takie samo jak w art. 268 § 2 k.k., co przesądza o identycznym rozumieniu tego terminu na gruncie obu przepisów.

Przestępstwo przewidziane w art. 269 k.k. ma alternatywnie określone znamiona opisujące czynność wykonawczą i może polegać na: zniszczeniu, uszkodzeniu lub zmianie zapisu informacji (art. 269 § 1 k.k.); zakłóceniu lub uniemożliwieniu automatycznego gromadzenia lub przekazywania informacji (art. 269 § 1 k.k.); zniszczeniu lub wymianie nośnika informacji albo na zniszczeniu lub uszkodzeniu urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przesyłania informacji (art. 269 § 2 k.k.). Pierwsza część znamion czynnościowych (niszczenie, uszkadzanie lub zmiana zapisu informacji) służy zabezpieczaniu integralności zapisów informacji o szczególnym znaczeniu. W tym zakresie różnica między przepisem art. 268 § 2 a prze-

[242] Identycznie W. Wróbel, *Uwagi wprowadzające...*, s. 1023; A. Adamski, *Przestępstwa komputerowe...*, s. 83.

[243] Zob. L. Gardocki, *Prawo karne*, Warszawa 1999, s. 293.

[244] Analogiczny warunek zawarty jest w § 303b StGB, gdzie wymaga się istotności przetwarzanych informacji dla przedsiębiorstwa, zakładu lub organu. W piśmiennictwie wskazuje się, że *„ob die Datenverarbeitung wesentliche Bedeutung für den Betrieb usw. hat, entscheidet sich nicht nach dem Umfang der Datenverarbeitung. Massgebend ist vielmehr, dass die Danetverarbeitung die für die Funktionsfähigkeit des betroffenen Betriebs usw. zentralen Informationen enthält, die Funktionsfähigkeit des Betriebs usw. also auf der Grundlage seiner konkreten Arbeitsweise, Ausstattung und Organisation ganz oder zu einem wesentlichen Teil von dem einwandfreien Finktionieren der Datenverarbeitung abhängt"* (W. Stree (w:) Schönke/Schröder, *Strafgesetzbuch. Kommentar...*, s. 1954).

[245] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1023; E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 207.

pisem art. 269 § 1 *in principio* sprowadza się do rodzaju informacji wyrażanej przez atakowany zapis zamieszczony na komputerowym nośniku informacji. Z uwagi na znacznie większe znaczenie informacji chronionej przez przestępstwo sabotażu komputerowego od informacji podlegającej ochronie na podstawie art. 268 § 2 k.k. oraz identyczność pozostałych znamion czynu zabronionego określonych w obu tych przepisach, a także biorąc pod uwagę różnicę w ustawowych granicach zagrożenia karą i środkami karnymi, stwierdzić należy, iż sabotaż komputerowy stanowi typ kwalifikowany przestępstwa naruszenia integralności informacji.[246]

Druga część znamion czynnościowych obejmuje zachowania polegające na zakłócaniu lub uniemożliwianiu automatycznego gromadzenia lub przekazywania informacji. Zdecydowany priorytet uzyskuje w kontekście tych znamion dostępność informacji o szczególnym znaczeniu.[247] Zakłócenie automatycznego gromadzenia lub przekazywania informacji obejmuje wszelkie czynności oddziałujące na procesy gromadzenia lub przekazywania, których skutkiem jest przerwanie tych procesów, ich zniekształcenie lub modyfikacja, chociażby obejmowała ona wyłącznie treść danych. Trzecia część znamion odnosi się do ataków skierowanych na nośniki informacji lub urządzenia służące do automatycznego przetwarzania, gromadzenia lub przesyłania informacji. Należy jednak podkreślić, iż mimo wskazania ustawodawcy na nośniki lub urządzenia służące do przetwarzania, gromadzenia i przesyłania informacji jako przedmiot bezpośredniego oddziaływania, relewantny z punktu widzenia znamion sabotażu komputerowego atak dokonywać się musi jednocześnie na nośnik lub urządzenie oraz zgromadzoną na nich informację o szczególnym znaczeniu. Pierwsza część znamion przestępstwa z art. 269 § 2 k.k., odnosząca się m.in. do niszczenia nośnika, wyraźnie nawiązuje do znamion przestępstwa określonego w art. 269 § 1 k.k. Posługując się sformułowaniem zawartym *in principio* w art. 268 § 2 k.k. „kto dopuszcza się czynu określonego w § 1", ustawodawca jednoznacznie przesądził, że zniszczenie lub wymienienie nośnika albo urządzenia służącego do przetwarzania, gromadzenia lub przesyłania informacji stanowić ma środek lub sposób dopuszczenia się czynu określonego w § 1, a więc zniszczenia, uszkodzenia,

[246] Co do techniczno-legislacyjnych sposobów budowy typów zmodyfikowanych zob. szerzej W. Wolter, *Reguły wyłączania wielości ocen w prawie karnym*, Warszawa 1961, s. 26 i n.; tenże, *Z rozważań nad kwalifikowanymi typami przestępstw*, Państwo i Prawo 1972, nr 8–9, s. 25 i n.; T. Bojarski, *Odmiany podstawowych typów przestępstw w polskim prawie karnym*, Warszawa 1982, s. 20 i n.; M. Dąbrowska-Kardas, P. Kardas, *Kryminalizacja ucieczki sprawcy wypadku drogowego z miejsca zdarzenia*, cz. I, Palestra 1996, Nr 3–4, s. 9–23.

[247] Por. L. Gardocki, *Prawo karne...*, s. 292; A. Adamski, *Przestępstwa komputerowe...*, s. 81.

usunięcia lub zmiany zapisu informacji o szczególnym znaczeniu albo zakłócenia lub uniemożliwienia automatycznego gromadzenia lub przekazywania tych informacji. Innymi słowy, nie stanowi realizacji znamion przestępstwa określonego w art. 269 § 2 k.k. takie zachowanie, które prowadzi do zniszczenia lub wymiany nośnika informacji albo do zniszczenia lub uszkodzenia urządzenia służącego do przetwarzania, gromadzenia lub przekazywania informacji, jeżeli jednocześnie sprawca nie zniszczył, nie uszkodził, nie usunął lub nie zmienił zapisu informacji o szczególnym znaczeniu bądź nie doprowadził do zakłócenia lub uniemożliwienia automatycznego gromadzenia czy przekazywania takich informacji.[248]

Przestępstwo określone w art. 269 k.k. może być popełnione tylko umyślnie, przy czym dopuszczalne jest działanie zarówno z zamiarem bezpośrednim, jak i wynikowym.[249]

PRZESTĘPSTWA KOMPUTEROWE ZAMIESZCZONE W ROZDZIALE XXXV PT. „PRZESTĘPSTWA PRZECIWKO MIENIU"

14. W rozdziale poświęconym ochronie jednego z najbardziej standardowych dóbr prawnych, jakim jest mienie, ustawodawca zamieścił pięć typów przestępstw, w których znamionach występuje albo specyficzne „komputerowe" dobro prawne podlegające ochronie (tak jest w przypadku art. 278 § 2 k.k. oraz art. 293 k.k. w zw. z art. 291 lub w zw. z art. 292 k.k.), albo specyficzny „komputerowy" sposób realizacji znamion przestępstwa nastawionego na ochronę tradycyjnych karnoprawnych wartości (tak jest w przypadku art. 287 k.k. oraz art. 285 k.k.). Z uwagi na ustawową charakterystykę znamion można zatem wymienione wyżej typy czynu zaliczyć do kategorii przestępstw komputerowych.

KRADZIEŻ PROGRAMU KOMPUTEROWEGO — ART. 278 § 2 K.K.

15. Ustawowa charakterystyka przestępstwa kradzieży uległa dosyć istotnym zmianom w nowym Kodeksie karnym w porównaniu do kształtu prze-

[248] Zob. W. Wróbel, *Uwagi wprowadzające...*, s. 1024–1025; E. Czarny-Drożdżejko, *Ochrona informacji...*, s. 209; O. Górniok (w:) *Kodeks karny...*, s. 326–327.

[249] Por. W. Wróbel, *Uwagi wprowadzające...*, s. 1025; O Górniok (w:) *Kodeks karny...*, s. 326–237.

stępstwa kradzieży określonego w art. 203 k.k. z 1969 r.[250] Opisujący znamiona kradzieży art. 278 k.k. z 1997 r. zawiera istotne modyfikacje w zakresie jurydycznego opisu tego przestępstwa. Po pierwsze, inaczej określony został przedmiot kradzieży, którym jest obecnie nie „cudze mienie ruchome", jak stanowił art. 203 k.k. z 1969 r., lecz „cudza rzecz ruchoma". Po drugie, do k.k. z 1997 r. wprowadzono dwa nieznane k.k. z 1969 r. typy kradzieży, polegające na kradzieży programu komputerowego oraz kradzieży energii elektrycznej i karty uprawniającej do podjęcia pieniędzy z automatu bankowego. Po trzecie, w k.k. z 1997 r. w art. 115 § 9 zawarto ustawową definicję pojęcia „rzecz ruchoma", wymieniając przedmioty uzyskujące z woli ustawodawcy walor rzeczy ruchomej w obszarze prawa karnego.[251] Wszystkie te zmiany mają istotne znaczenie dla wykładni znamion nowej odmiany kradzieży, nazywanej dość powszechnie w piśmiennictwie karnistycznym „kradzieżą programu komputerowego".[252] Została ona uregulowana w art. 278 § 2 k.k., który stanowi, że karze przewidzianej za kradzież (tj. w art. 278 § 1 k.k.) podlega także ten, „kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej".[253] Wprowadzenie specjalnej regulacji odnoszącej się do „kradzieży" programu komputerowego wynika z kilku powodów, wśród których dwa wydają się mieć szczególne znaczenie. Pierwszy związany jest ze szczególnym statusem programu komputerowego, który nie będąc przedmiotem materialnym nie może być uznany za rzecz.[254] Drugi powód związany jest z normatywną charakterysty-

[250] Zob. szerzej M. Dąbrowska-Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 29–33; B. Michalski, *Przestępstwa przeciwko mieniu...*, s. 43–45; O. Górniok, *Komentarz...*, s. 342–346.

[251] Przyjęta w art. 115 § 9 k.k. stylistyka pozwala stwierdzić, iż zawarte w tym przepisie wyliczenie przedmiotów uznawanych na gruncie polskiego prawa karnego jako rzeczy ruchome ma charakter przykładowy. Przesądza o tym, moim zdaniem, zamieszczone *in principio* w art. 115 § 9 sformułowanie „rzeczą ruchomą lub przedmiotem jest także...". Zob. szerzej w tej kwestii M. Dąbrowska-Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 41 i n.; A. Wąsek (w:) M. Kalitowski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny. Komentarz*, t. II, Gdańsk 1999, s. 388–389; A. Zoll (w:) K. Buchała, A. Zoll, *Kodeks karny. Część ogólna. Komentarz*, Kraków–Zakamycze 1998, s. 630–631.

[252] Nazwą tą posługują się m.in.: E. Czarny-Drożdżejko, *Ochrona informacji...*, s. 208 i n.; O. Górniok (w:) *Kodeks karny...*, s. 343. Natomiast A. Adamski i L. Gardocki określają to przestępstwo jako „bezprawne uzyskanie programu komputerowego" — zob. A. Adamski, *Przestępstwa komputerowe...*, s. 111 i n.; L. Gardocki, *Prawo karne...*, s. 298.

[253] Przepis ten nie posiada odpowiednika w niemieckim kodeksie karnym, w którym kradzież określona została w sposób tradycyjny, bez wprowadzania przez ustawodawcę szczególnych regulacji odnoszących się do programu komputerowego. Kryminalizacja bezprawnego zaboru programu komputerowego zawarta jest w niemieckiej ustawie o prawie autorskim w § 108. Zob. szerzej w tej kwestii U. Sieber, *Przestępczość komputerowa...*, s. 233 i n. Zob. też § 242 i § 243 StGB.

[254] Zob. E. Czarny-Drożdżejko, *Ochrona informacji...*, s. 209–210; M. Dąbrowska-Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 29–32, 53 i n.

ką klasycznej kradzieży, która polega na zaborze cudzej rzeczy ruchomej w celu przywłaszczenia. Jej istotą jest więc wyjęcie rzeczy spod władztwa dotychczasowego dysponenta i przejęcie tego władztwa przez zamachowca. Tymczasem w przypadku czynności dokonywanych na programach komputerowych co do zasady przejęcie programu nie oznacza odebrania władztwa nad programem osobie dotychczas nim władającej.[255] Oba te powody sprawiały, że kwalifikowanie przypadków bezprawnego uzyskania programu komputerowego jako zwykłej kradzieży było niezwykle utrudnione, a w pewnej grupie przypadków w ogóle niemożliwe. Wprowadzenie do nowego Kodeksu karnego szczególnego przepisu, odnoszącego się do przypadków powszechnie nazywanych kradzieżą programów komputerowych, stanowi próbę wypełnienia luki prawnej w tej sferze regulacji.[256] Uregulowanie bezprawnego uzyskania programu komputerowego w odrębnym przepisie, uwzględniającym w jurydycznej charakterystyce przestępstwa jego odmienności w stosunku do klasycznej kradzieży, powoduje, iż znamiona typu czynu zabronionego określonego w art. 278 § 2 k.k. dosyć istotnie różnią się od znamion kradzieży rzeczy ruchomej określonych w art. 278 § 1 k.k. Przestępstwo kradzieży programu komputerowego inaczej niż zwykła kradzież określa przedmiot ochrony oraz odmiennie charakteryzuje znamię czynności wykonawczej. Ponadto ustawodawca wprowadził w opisie typu kradzieży programu komputerowego szczególną przesłankę odnoszącą się do strony podmiotowej, nie występującą w typie kradzieży zwykłej, wymagając dla odpowiedzialności karnej dzia-

[255] Zob. szerzej M. Dąbrowska-Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 54.

[256] Luka ta, od wejścia w życie ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, nie była bardzo szeroka, albowiem art. 117 tejże ustawy przewiduje typ czynu zabronionego, który w pewnym zakresie obejmuje kryminalizacją zachowania odpowiadające istocie kradzieży programu komputerowego. Jednak z uwagi na fakt, iż penalizacja bezprawnego uzyskania programu komputerowego na podstawie art. 117 prawa autorskiego z jednej strony nie obejmuje wszystkich przypadków stanowiących w istocie kradzież programu (użyty w art. 278 § 2 k.k. zwrot „uzyskuje" oznacza znacznie szerszy krąg zachowań niż wymienione w art. 117 ustawy prawo autorskie sformułowania „utrwala" oraz „zwielokrotnia"), z drugiej obłożona jest swoistym warunkiem podmiotowym w postaci godzenia się sprawcy na rozpowszechnianie utrwalonego lub zwielokrotnionego programu komputerowego, znacznie ograniczającym krąg zachowań karalnych, wprowadzenie szczególnej regulacji odnoszącej się do kradzieży programu komputerowego było konieczne. Inna sprawa, iż wzajemne relacje przepisów art. 278 § 2 k.k. i art. 117 ustawy o prawie autorskim i prawach pokrewnych nie zostały przez ustawodawcę zakreślone w sposób zadowalający. Kwestie te będą przedmiotem szczegółowej analizy w dalszej części niniejszego opracowania. Zob. szerzej w tej kwestii M. Dąbrowska-Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 29–33 i 53–59; M. Dąbrowska-Kardas, P. Kardas (w:) *Kodeks karny. Część szczególna...*, s. 7 i n.; B. Michalski, *Przestępstwa przeciwko mieniu*, Warszawa 1999, s. 74 i n.; O. Górniok (w:) *Kodeks karny...*, s. 343 i n.; Z. Ćwiąkalski (w:) J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, Warszawa 1995, s. 486–489.

łania sprawcy w celu osiągnięcia korzyści majątkowej. Wymienione wyżej odmienności w ustawowej charakterystyce znamion przestępstwa kradzieży programu komputerowego sprawiają, że ich wykładnia z jednej strony wymaga specyficznego, interdyscyplinarnego podejścia, z drugiej zaś, ze względu na wprowadzenie do znamion pojęć integralnie związanych z nowoczesnymi technologiami gromadzenia i przetwarzania danych, rodzi znacznie poważniejsze trudności interpretacyjne niż klasyczna kradzież.

Przedmiotem przestępstwa przewidzianego w art. 278 § 2 k.k. jest program komputerowy. W polskim ustawodawstwie brak jest legalnej definicji tego pojęcia.[257] W języku potocznym, wykorzystującym dorobek współczesnej informatyki, przez program komputerowy rozumie się „algorytm wraz ze strukturami danych, na których operuje; przepis, według którego komputer wykonuje czynności przewidziane w algorytmie".[258] Z prawnego punktu widze-

[257] Definicji pojęcia „program komputerowy" nie zawiera także ani Dyrektywa Rady EWG z dnia 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych, ani oparta na niej w zakresie ochrony programów komputerowych ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych. Jak podkreślają J. Barta i R. Markiewicz, twórcy ustawy uznali, że „postęp techniczny istniejący w sferze informatyki spowodować mógłby w szybkim czasie nieadekwatność ustawowej definicji w odniesieniu do zmieniającej się w tym zakresie rzeczywistości" (w: *Komentarz do ustawy o prawie autorskim...*, s. 348). Zob. też B. Michalski, *Przestępstwa przeciwko mieniu...*, s. 74; E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 210 i n.; A. Adamski, *Przestępstwa komputerowe...*, s. 111 i n. Należy jednak podkreślić, iż w niektórych ustawodawstwach, zwłaszcza w ustawach autorskich, podawane są jurydyczne definicje programu komputerowego jako szczególnego przedmiotu ochrony. Jak podkreślają J. Barta i R. Markiewicz, w ustawach autorskich obcych porządków prawnych program komputerowy „określany jest najczęściej jako zakodowana sekwencja instrukcji (rozkazów) wykonywanych bezpośrednio lub pośrednio przez komputer lub inne urządzenie zdolne do przetwarzania informacji w celu uzyskania określonego rezultatu (realizacji określonych funkcji lub zadań)" (*Główne problemy prawa komputerowego...*, s. 20). Przegląd ustawowych definicji programów komputerowych zawiera opracowanie M.S. Kepplinger, *International Protection for Computer Programs*, Software Law Journal 1990, nr 1, s. 15–18.

[258] Takim określeniem posługuje się B. Michalski, *Przestępstwa przeciwko mieniu...*, s. 75 oraz O. Górniok (w:) *Kodeks karny...*, s. 343. W *Słowniku języka polskiego...*, t. II, s. 890, program komputerowy zdefiniowany jest jako „ciąg instrukcji napisanych w języku zrozumiałym dla komputera, pozwalających wykonać jakąś operację, np. przetwarzanie tekstów, obrazów, wykonywanie obliczeń". Natomiast w definicji przyjętej przez Międzynarodową Organizację Własności Intelektualnej (WIPO) program komputerowy to „zbiór instrukcji (kodów źródłowych), który po umieszczeniu na rozpoznawalnym przez maszynę nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tej maszyny (kod wynikowy) powoduje, że osiąga ona zdolność do wykonywania czynności lub też wykonuje daną czynność" (World Intellectual Property Organization (WIPO), *Model Provision on the Protection of Computer Software*, Genewa 1978, s. 35). Zob. też w tej kwestii A. Adamski, *Przestępstwa komputerowe...*, s. 112. K. Golat i R. Golat definiują program komputerowy jako „logicznie uporządkowany ciąg instrukcji, przeznaczony do uzyskiwania za pośrednictwem sprzętu komputerowego pożądanego przez użytkownika systemu komputerowego wyniku" (*Prawo komputerowe — zagadnienia podstawowe*, Warszawa 1998, s. 22).

nia pojęcie „program komputerowy" odsyła karnistę do regulacji zawartych w ustawie z dnia 23 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. Nr 43, poz. 170, ze zm.). Zawarty w rozdziale VII tej ustawy, zatytułowanym „Przepisy szczególne dotyczące programów komputerowych", przepis art. 74 ust. 1 stanowi, że „programy komputerowe podlegają ochronie jako utwory literackie, o ile przepisy niniejszego rozdziału nie stanowią inaczej". Wedle ust. 2 art. 74 tej ustawy, „ochrona przyznana programowi komputerowemu obejmuje wszystkie formy jego wyrażenia, w tym wszystkie formy dokumentacji projektowej, wytwórczej i użytkowej. Idee i zasady, będące podstawą jakiegokolwiek elementu programu komputerowego, w tym podstawą łączy, nie podlegają ochronie". Program komputerowy podlega zatem specjalnej ochronie ustanowionej w ustawie o prawie autorskim i prawach pokrewnych. Należy jednak zaznaczyć, że ochroną prawnoautorską objęte są tylko takie programy komputerowe, które stanowią dzieło w rozumieniu tej ustawy. Wynika to jednoznacznie z brzmienia jej art. 74 ust. 1 w zw. z art. 1 ust. 2 pkt 1 tej ustawy, który uznaje program komputerowy za odrębny rodzaj utworu, m.in. w stosunku do utworu naukowego i literackiego.[259] Pierwszy z powołanych przepisów przyznaje programom komputerowym ochronę taką, jaka przysługuje utworom literackim, drugi — określa przedmiot prawa autorskiego jako „każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór)", wskazując przykładowe przedmioty prawa autorskiego jako utwory „wyrażone słowem, symbolami matematycznymi, znakami graficznymi (literackie, publicystyczne, naukowe, kartograficzne oraz programy komputerowe)". Ustawa o prawie autorskim, nie definiując pojęcia „program komputerowy", wprowadza zasadę ochrony tylko takich programów, które mają charakter utworu, innymi słowy — stanowią przejaw działalności twórczej o indywidualnym charakterze. Artykuł 278 § 2 k.k. także nie zawiera definicji pojęcia „program komputerowy", zarazem jednak nie wyraża wprost żadnego ograniczenia zakresu ochrony przewidzianej dla tych programów, w tym w szczególności literalnie nie zawęża jej jedynie do programów stanowiących dzieła w rozumieniu prawa autorskiego.[260] Zestawiając ze sobą przepisy ustawy o prawie autorskim i prawach pokrewnych odnoszące się do ochrony programów komputerowych z treścią art. 278 § 2 k.k., konieczne jest rozstrzygnięcie zagadnienia zakresu przedmiotowego ochro-

[259] Zob. szerzej J. Barta, R. Markiewicz (w:) *Komentarz do ustawy o prawie autorskim...*, s. 48–57 i 349 i n.

[260] Por. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 210–211.

ny przewidzianej w art. 278 § 2 k.k. W tej kwestii prezentowane są w piśmiennictwie dwa stanowiska.

Pierwsze (nazwijmy je tutaj autonomicznym) zakłada, iż treść art. 278 § 2 k.k. stanowi samodzielną podstawę do określenia przedmiotowego zakresu ochrony. Zwolennicy tego ujęcia przyjmują, że przepis art. 278 § 2 k.k., posługując się jedynie pojęciem „program komputerowy" bez jakiegokolwiek bliższego określenia, nie wskazuje na żadne związki prawnokarnej ochrony programów komputerowych z zakresem ochrony prawnoautorskiej. Oznacza to, iż niezależnie od charakteru programu komputerowego — a zatem w całkowitym oderwaniu od tego, czy program stanowi przejaw twórczości o indywidualnym charakterze, czy też nie — decydujące dla przyznania mu prawnokarnej ochrony jest przesądzenie, iż określony wytwór intelektu jest programem komputerowym i stanowi element czyjegoś mienia. Jako składnik mienia będący dobrem niematerialnym, jest jednocześnie prawem majątkowym i zalicza się do kręgu desygnatów definicji mienia z art. 44 Kodeksu cywilnego, co przesądza o jego prawnokarnej ochronie na mocy art. 278 § 2 k.k.[261]

Stanowisko drugie (nazwijmy je tutaj subsydiarnym) wychodząc z zasady subsydiarności prawa karnego przyjmuje, że przepis art. 278 § 2 k.k. może przyznawać programom komputerowym ochronę co najwyżej w takim zakresie, jaki objęty jest regulacją innych działów prawa, regulujących bezpośrednio zasady postępowania i obrotu tym szczególnym rodzajem dobra prawnego. Opierając się na cywilistycznej zasadzie *numerus clausus* praw bezwzględnych[262] i zaliczając do tej kategorii praw prawo do dobra niematerialnego, jakim jest program komputerowy, wskazuje się na bezpośredni związek ochrony karnoprawnej z zakresem ochrony przewidzianej dla tego dobra w innych przepisach prawa. Ponieważ regulacja związana z ochroną programów komputerowych zawarta w prawie autorskim ograniczona jest od strony przedmiotowej jedynie do takich programów, które mają charakter twórczy (są utworami), to w świetle tego działu prawa program komputerowy nie stanowiący dzieła nie podlega prawnej ochronie. Jeśli zatem program komputerowy nie będący dziełem nie jest chroniony na gruncie prawa autorskiego, to brak jest podstaw do przyznawania mu ochrony w prawie karnym, które pełni w stosunku do pozostałych działów prawa ewidentnie subsydiarną funkcję. Należy jednak podkreślić, że rozumowanie ograniczające zakres ochrony przewidziany w art. 278 § 2 k.k. jedynie do programów komputerowych spełniających cechy utworu oparte jest na założeniu, iż prawo do programu komputerowego jako dobra niematerialnego ma charakter prawa bezwzględnego. Tylko bowiem przy przyjęciu tego założenia możliwe jest ograniczanie kręgu tych praw poprzez odwołanie się do zasady *numerus clausus*.[263] Przyjęcie stanowiska, wedle którego prawo do programu komputerowego jako dobra niematerialnego ma charakter względny, wyłącza obowiązywanie w tym zakresie zasady *numerus clausus*, stwarzając tym samym podstawy do tworzenia nowych praw.[264] Wybór jednego z alternatywnych sposobów wykładni znamion przestępstwa z art. 278 § 2 k.k. uzależniony jest więc od rozstrzygnięcia zagadnienia *stricte* cywilistycznego, związanego z pytaniem o charakter prawa do dobra niematerialnego w postaci programu komputerowego.[265] Przyjęcie tezy, iż prawo to zalicza się do kategorii praw bezwzględnych implikuje, że jego ochrona, z uwagi na zasadę *numerus clausus*, musi być wyraźnie uregulowana w obowiązujących przepisach prawa.[266] Brak takiej szczególnej regulacji oznacza zarazem brak ochrony w obszarze pozakarnym i jednocześnie stanowi podstawową przeszkodę w przyznaniu ochrony prawnokarnej w tym zakresie z uwagi na zasadę subsydiarności prawa karnego. Przychylenie się do koncepcji uznającej prawa do dobra niematerialnego w postaci programu komputerowego za prawo względne wyłącza zastosowanie zasady *numerus clausus* w odniesieniu do podstaw ochrony tego prawa. W takim wypadku istnieje możliwość ochrony programów komputerowych nie stanowiących przedmiotu ochrony w świetle prawa autorskiego w oparciu o ogól-

[261] Rozumowanie takie prezentuje E. Czarny–Drożdżejko, zaznaczając jednak, iż w doktrynie prawa karnego przeważyć może pogląd odmienny (*Ochrona informacji...*, s. 211).

[262] Por. Z. Radwański, *Prawo cywilne — część ogólna*, Warszawa 1995, s. 74 i n.

[263] E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 211.

[264] Tak np. zdaniem K. Golat i R. Golat, ochrona interesów majątkowych związanych z programami komputerowymi, które nie podlegają ochronie prawa autorskiego wyznaczana jest przez regulacje cywilnoprawne (*Prawo komputerowe...*, s. 183 i n.). Zob. też A. Adamski, *Przestępstwa komputerowe...*, s. 114; E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 211–212.

[265] Zob. szerzej S. Grzybowski (w:) *System prawa cywilnego. Część ogólna*, red. S. Grzybowski, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1985, s. 231–233 i s. 439 i n.; Z. Radwański, *Prawo cywilne...*, s 74 i n.; J. Barta, R. Markiewicz (w:) *Komentarz do ustawy o prawie autorskim...*, s. 348 i n.

[266] Kwestia charakteru prawa do programu komputerowego jest wyjątkowo sporna jeśli postrzega się ją w kontekście statusu i charakteru prawa do dóbr niematerialnych. Zob. szerzej w tej kwestii S. Grzybowski, *Umowy know–how na tle kodeksu cywilnego*, Krakowskie Studia Prawnicze 1968, z. 1–2, s. 35 i n.; S. Sołtysiński, *Charakter praw wynalazcy*, Poznań 1967, s. 25 i n.; tenże, *Licencje na korzystanie z cudzych rozwiązań technicznych*, Warszawa 1970, s. 12 i n.; B. Gawlik, *Umowa know–how. Zagadnienia konstrukcyjne*, Zeszyty Naukowe UJ, *Prace z Wynalazczości i Ochrony Własności Intelektualnej*, z. 2, Warszawa–Kraków 1974, s. 30 i n.; tenże, *Know–how* (w:) *Prawo wynalazcze*, red. S. Grzybowski i A. Kopff, Warszawa 1978, s. 368 i n.; M. Poźniak–Niedzielska, *Dobra niematerialne przedsiębiorstwa państwowego*, Warszawa–Łódź 1990, s. 26 i n.

ne regulacje prawa cywilnego[267] i w konsekwencji nie ma przeszkód w przyznaniu programom komputerowym ochrony na podstawie art. 278 § 2 k.k. w pełnym zakresie, bez naruszenia zasady subsydiarności prawa karnego. W powyższej perspektywie widać dość dobrze, że problem przedmiotowego zakresu ochrony czynu zabronionego określonego w przepisie art. 278 § 2 k.k. rodzi poważne wątpliwości,[268] u podłoża których leżą jednak nie karnistyczne, lecz cywilistyczne kontrowersje. W tym stanie rzeczy trudno oczekiwać od karnisty jednoznacznego stanowiska w tej sprawie. Nie podejmując próby rozstrzygnięcia ściśle cywilistycznego zagadnienia charakteru prawa do dobra niematerialnego w postaci programu komputerowego, pozostaje w tym miejscu jedynie stwierdzić, że program komputerowy stanowiący przejaw działalności twórczej o indywidualnym charakterze (a więc będący utworem w rozumieniu prawa autorskiego) stanowi zawsze przedmiot podlegający ochronie na podstawie art. 278 § 2 k.k.[269] Natomiast problem ochrony programu komputerowego nie będącego utworem na podstawie art. 278 § 2 k.k. rozstrzygać należy w oparciu o uprzednie przesądzenie charakteru praw do tego programu.

Czynność wykonawcza przestępstwa kradzieży programu komputerowego określona została jako uzyskanie bez zgody osoby uprawnionej cudzego programu komputerowego. Użyte w analizowanym przepisie sformułowanie „bez zgody osoby uprawnionej" wskazuje na charakterystykę zachowania karalnego, które, identycznie jak w przypadku zwykłej kradzieży, dokonuje się wbrew woli osoby uprawnionej.[270] Odpowiedź na pytanie, kim w rzeczywistości jest osoba uprawniona i jakiego rodzaju prawa do programu komputerowego stanowiącego przedmiot przestępstwa może ona posiadać, uzależniona jest od rozstrzygnięcia kwestii charakteru praw do programu komputerowego. Jeśli bowiem przyjmie się stanowisko, że prawa te zo-

[267] Przede wszystkim na podstawie art. 415 k.c. i n. (określających zasady odpowiedzialności deliktowej), przepisów art. 336 i n. k.c. — dotyczących ochrony posiadania itp. Zob. w tej kwestii B. Gawlik, *Umowa know-how*..., s. 58–74; K. Golat, R. Golat, *Prawo komputerowe*..., s. 183 i n. Zob. też A. Adamski, *Przestępstwa komputerowe*..., s. 114; E. Czarny–Drożdżejko, *Ochrona informacji*..., s. 212.

[268] O tych i innych jeszcze problemach związanych z przedmiotem ochrony kradzieży programu komputerowego pisał jeszcze w trakcie prac nad projektem Kodeksu karnego K. Buchała (*Reforma polskiego prawa karnego materialnego* (w:) *Przestępczość komputerowa*, red. A. Adamski, Poznań 1994, s. 129 i n.).

[269] Por. M. Dąbrowska–Kardas, P. Kardas, *Przestępstwa przeciwko mieniu*..., s. 53; A. Adamski, *Przestępstwa komputerowe*..., s. 114–115; O. Górniok (w:) *Kodeks karny*..., s. 342–344; B. Michalski, *Przestępstwa przeciwko mieniu*..., s. 74–76; E. Czarny–Drożdżejko, *Ochrona informacji*..., s. 210 i n.

[270] Por. M. Dąbrowska–Kardas, P. Kardas, *Przestępstwa przeciwko mieniu*..., s. 55.

stały w sposób wyczerpujący opisane w ustawie o prawie autorskim i prawach pokrewnych (zasada *numerus clausus*), wówczas uprawnienie do dysponowania tym programem przysługiwać może twórcy programu (art. 8 ust. 1 prawa autorskiego) lub pracodawcy, jeżeli program komputerowy stworzony został przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy i umowa o pracę nie stanowi inaczej (art. 74 ust. 3 prawa autorskiego).[271] Osobą uprawnioną może być także nabywca programu komputerowego jako utworu, jeżeli twórca lub pracodawca przenieśli na tę osobę autorskie prawa majątkowe.[272] Jeżeli natomiast przyjmie się koncepcję względności praw do programu komputerowego, wówczas uprawnionym do dysponowania takim programem niestanowiącym utworu będzie każda osoba, która posiada do programu prawo własności lub inne prawo rzeczowe albo obligacyjne.[273]

Sama czynność wykonawcza, określona jako „uzyskanie", zgodnie ze słownikowym znaczeniem oznacza „wejście w posiadanie czegoś pożądanego, osiągnięcie czegoś, zdobycie czegoś".[274]

Uzyskanie w kontekście, w jakim użyte zostało w znamionach przestępstwa kradzieży programu komputerowego rozumiane być powinno jako bezprawne zdobycie przez sprawcę programu komputerowego. Jak podkreśla E. Czarny–Drożdżejko, pojęcie „uzyskuje" budzić może poważne wątpliwości interpretacyjne w kontekście regulacji zawartych w ustawie o prawie autorskim i prawach pokrewnych. Ustawa ta bowiem w ogóle nie posługuje się terminem „uzyskuje", używa natomiast kilku zwrotów o zbliżonym znaczeniu, takich jak „zwielokrotnia", „utrwala", „wprowadza do pamięci komputera".[275] „Zwielokrotnienie" oznacza na gruncie prawa autorskiego wytworzenie egzemplarzy dzieła, które stanowią podstawę do zapoznania się z nim w sposób bezpośredni lub przy użyciu specjalnego urządzenia.[276] „Utrwalenie" to stworzenie egzemplarza utworu. Trafnie wskazuje E. Czarny–Drożdżejko, że uzyskanie oznaczać może zarówno utrwalenie programu

[271] Zob. szerzej J. Barta, R. Markiewicz (w:) *Komentarz do ustawy o prawie autorskim*..., s. 351–352.

[272] Por. E. Czarny–Drożdżejko, *Ochrona informacji*..., s. 212; J. Barta, R. Markiewicz (w:) *Komentarz do ustawy o prawie autorskim*..., s. 225 i n.

[273] Zob. M. Dąbrowska–Kardas, P. Kardas, *Przestępstwa przeciwko mieniu*..., s. 55; E. Czarny–Drożdżejko, *Ochrona informacji*..., s. 213; B. Michalski, *Przestępstwa przeciwko mieniu*..., s. 76.

[274] *Słownik języka polskiego*..., s. 598.

[275] Pojęcia te występują w art. 50 ustawy o prawie autorskim i prawach pokrewnych, który wymienia odrębne pola eksploatacji. Co do znaczenia tych terminów zob. szerzej J. Barta, R. Markiewicz (w:) *Komentarz do ustawy o prawie autorskim*..., s. 246 i n.

[276] Por. J. Barta, R. Markiewicz (w:) *Komentarz do ustawy o prawie autorskim*..., s. 248; E. Czarny–Drożdżejko, *Ochrona informacji*..., s. 214.

komputerowego, jak i jego zwielokrotnienie.[277] Pojęcie „uzyskanie" nie ogranicza się bowiem jedynie do zaboru nośnika, na którym zapisany i przechowywany jest program komputerowy (np. dyskietki, CD, twardego dysku komputera lub całego komputera, na którym zapisany jest program), chociaż w wielu wypadkach czynność wykonawcza dokonywana będzie właśnie w ten sposób.[278] Określenie czynności wykonawczej jest więc na gruncie art. 278 § 2 k.k. znacznie szersze niż w przepisie art. 117 ustawy o prawie autorskim i prawach pokrewnych, z tym jednak, że czynności charakteryzujące przestępstwo z art. 117 ustawy o prawie autorskim i prawach pokrewnych zawierają się w pojęciu „uzyskuje" występującym w art. 278 § 2 k.k.[279] Ze względu na technologiczne właściwości programu komputerowego, będącego w istocie matematycznym zapisem informacji na odpowiednim nośniku, posiadającym właściwość wielokrotnego kopiowania, któremu nie towarzyszy naruszenie pierwotnej substancji programu, bezprawne uzyskanie programu komputerowego co do zasady nie będzie połączone z zaborem nośnika, na którym jest on zapisany, skutkującym pozbawienie osoby uprawnionej możliwości korzystania z tego programu. Uzyskanie, jako znamię przestępstwa kradzieży programu komputerowego, nie musi łączyć się z pozbawieniem osoby uprawnionej władztwa nad programem, lecz może przybierać postać m.in. kopiowania programu lub wszelkich innych form nielegalnego wejścia w posiadanie takiego programu.[280]

Z punktu widzenia strony podmiotowej, czyn zabroniony określony w art. 278 § 2 k.k. musi być popełniony umyślnie, przy czym ustawa wymaga, aby sprawca działał ponadto w celu osiągnięcia korzyści majątkowej. Treść i zakres pojęcia „korzyść majątkowa" kształtowane są od wielu lat przez orzecznictwo i doktrynę prawa karnego, stąd w tym miejscu wystarczy zrekapitulować tylko powszechnie akceptowane ujęcie tej kwestii. Jako konstytutywne dla korzyści majątkowej wskazuje się takie cechy, jak: zdolność do zaspokajania przede wszystkim potrzeb materialnych, wartość ekonomiczna dająca się określić w kwocie pieniężnej, zmiana w stanie majątkowym osoby, która ją uzyskuje, wyrażająca się zwiększeniem aktywów lub zmniejszeniem pasy-

[277] E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 214.; J. Barta, R. Markiewicz (w:) *Komentarz do ustawy o prawie autorskim...*, s. 248 i n.

[278] Tak również B. Michalski, *Przestępstwa przeciwko mieniu...*, s. 76; O. Górniok (w:) *Kodeks karny...*, s. 343.

[279] W odniesieniu do charakterystyki znamion czynnościowych w przestępstwie z art. 117 ustawy o prawie autorskim i prawach pokrewnych zob. Z. Ćwiąkalski (w:) *Komentarz do ustawy o prawie autorskim...*, s. 488–489.

[280] Por. O. Górniok (w:) *Kodeks karny...*, s. 344; B. Michalski, *Przestępstwa przeciwko mieniu...*, s. 76; A. Adamski, *Przestępstwa komputerowe...*, s. 116 i n.

wów. Do korzyści majątkowej włącza się współczesne i przyszłe przysporzenia majątkowe, spodziewane korzyści majątkowe, ogólne polepszenie sytuacji majątkowej, a także uzyskanie możliwości pracy i godziwego zarobku.[281] Należy przypomnieć, że Kodeks karny z 1997 r. w art. 115 § 4 stanowi, iż korzyść majątkowa oznacza korzyść zarówno dla sprawcy, jak i dla osoby fizycznej lub prawnej, jednostki organizacyjnej nie posiadającej osobowości prawnej lub grupy osób prowadzącej zorganizowaną działalność przestępczą.

Ustawowy wymóg działania sprawcy kradzieży programu komputerowego w celu osiągnięcia korzyści majątkowej przesądza, iż czyn ten popełnić można tylko z zamiarem bezpośrednim. Co więcej, należy on do szczególnej kategorii przestępstw umyślnych, określanych w doktrynie mianem tzw. przestępstw kierunkowych.[282] Charakterystyczny dla strony podmiotowej przestępstwa z art. 278 § 2 k.k. zamiar bezpośredni musi obejmować zarówno cel działania sprawcy, jak i sposób działania prowadzący do tego celu. Sprawca powinien mieć pełną świadomość, że jego zachowanie stanowi uzyskiwanie bez zgody osoby uprawnionej programu komputerowego i chcieć tego. Jednocześnie sprawca musi byc w pełni świadomym tego, że jego działanie ma doprowadzić do osiągnięcia korzyści majątkowej i w tym celu je realizować. Cel osiągnięcia korzyści majątkowej powinien towarzyszyć realizacji każdego ze znamion strony przedmiotowej przestępstwa. Poszczególne elementy strony przedmiotowej przestępstwa kradzieży programu komputerowego, a więc fakt braku zgody osoby uprawnionej oraz działanie polegające na uzyskiwaniu programu komputerowego, muszą znaleźć odzwierciedlenie w świadomości sprawcy (w postaci tzw. pełnej świadomości) oraz być objęte jego wolą (tzw. chęcią ich wypełnienia). Warto podkreślić, że stosunkowo rygorystyczne ustawowe wymagania dotyczące strony podmiotowej przestępstwa sprawiają, że w sytuacji, gdy sprawca nie obejmuje świadomością któregoś z elementów strony przedmiotowej stwierdzić należy, iż nie zostają spełnione subiektywne warunki odpowiedzialności karnej. W takim przypadku bowiem sprawca nie tyle chce popełnić czyn zabroniony, co jedynie godzi się na jego popełnienie, zaś zamiar wynikowy jest wykluczony w odniesieniu do analizowanego przestępstwa.[283]

[281] Zob. w tej kwestii w szczególności O. Górniok, *O pojęciu „korzyści majątkowej" w kodeksie karnym (problemy wybrane)*, Państwo i Prawo 1978, nr 4, s. 115 i n.; J. Waszczyński, *O „korzyści majątkowej" w prawie karnym (problemy kodyfikacji)*, Państwo i Prawo 1981, nr 1, s. 65 i n.; J. Bednarzak, *Przestępstwo oszustwa w polskim prawie karnym*, Warszawa 1971, s. 85 i n.

[282] Zob. szerzej S. Frankowski, *Przestępstwa kierunkowe...*, s. 23 i n.

[283] Por. następujące orzeczenia Sądu Najwyższego: wyrok SN z 22 listopada 1973 r., III KR 278/73, OSNPG 1974, nr 7, poz. 81; wyrok SN z 20 lutego 1974 r., V KR 49/74, OSNKW 1974, nr 7, poz. 138.

Programy komputerowe stanowią także przedmiot prawnokarnej ochrony w świetle ustawy o prawie autorskim i prawach pokrewnych. Wymieniany wielokrotnie w tym opracowaniu art. 117 ust. 1 tej ustawy stanowi: „Kto bez uprawnienia albo wbrew jego warunkom utrwala lub zwielokrotnia cudzy utwór w wersji oryginalnej lub w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, godząc się na ich rozpowszechnianie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Typ kwalifikowany, określony w art. 117 ust. 2 ustawy o prawie autorskim i prawach pokrewnych, jako okoliczność kwalifikującą przyjmuje uczynienie sobie z popełniania przestępstwa określonego w art. 117 ust. 1 stałego źródła dochodu albo kierowanie lub organizowanie taką działalnością przestępną. Zakresy zastosowania norm sankcjonujących zdekodowanych z przepisu art. 278 § 2 k.k. i art. 117 ust. 1 i 2 ustawy o prawie autorskim i prawach pokrewnych w znacznej części się krzyżują.[284] Przedmiotem ochrony przepisu art. 117 prawa autorskiego jest cudzy utwór, przez który na gruncie tej ustawy rozumie się także program komputerowy. W tym zakresie zatem oba przepisy mają albo identyczną treść (jeśli wybierze się ujęcie, wedle którego art. 278 § 2 k.k. przydaje ochronę jedynie takim programom komputerowym, które są utworami), albo art. 278 § 2 k.k. obejmuje ochroną szerszy zakres niż art. 117 ustawy o prawie autorskim i prawach pokrewnych (jeśli wybierze się ujęcie, wedle którego odnosi się on do programów komputerowych będących utworami oraz do programów komputerowych nie będących utworami). Czynność wykonawcza przestępstwa opisanego w art. 117 prawa autorskiego polega na utrwalaniu lub zwielokrotnianiu utworu (programu komputerowego). Obie te formy, jak starano się to zilustrować powyżej, stanowią przypadki uzyskania programu komputerowego w rozumieniu art. 278 § 2 k.k. Przepis art. 117 prawa autorskiego dla odpowiedzialności karnej wymaga, aby sprawca, dopuszczając się jednej z alternatywnie scharakteryzowanych czynności, godził się jednocześnie na rozpowszechnianie utrwalanego lub zwielokrotnianego utworu; nie wymaga natomiast działania sprawcy w celu osiągnięcia korzyści majątkowej, jak czyni to art. 278 § 2 k.k. Istotna różnica między czynem zabronionym opisanym w art. 278 § 2 k.k. a czynem zabronionym przewidzianym w art. 117 ustawy o prawie autorskim i prawach pokrewnych sprowadza się więc do kształtu strony podmiotowej. Kradzież programu komputerowego (art. 278 § 2 k.k.) jest przestępstwem kierunkowym, wymagającym działania sprawcy w celu osiągnięcia korzyści majątkowej,

[284] Zob. A. Adamski, *Przestępstwa komputerowe...*, s. 120–121; E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 216–217.

natomiast przestępstwo z art. 117 ustawy o prawie autorskim i prawach pokrewnych jest przestępstwem umyślnym (dopuszczalna jest forma obu odmian umyślności), z tym jednak, iż wymaga ono co najmniej godzenia się sprawcy na rozpowszechnianie utrwalonego lub zwielokrotnionego utworu. Z tego punktu widzenia uzasadnione jest posługiwanie się w odniesieniu do przestępstwa z art. 117 prawa autorskiego nazwą „piractwo komputerowe".[285] Istota dodatkowego elementu strony podmiotowej przestępstwa ujętego w art. 117 ustawy o prawie autorskim i prawach pokrewnych, określonego jako godzenie się na rozpowszechnianie utrwalonego lub zwielokrotnionego programu komputerowego, sprowadza się do występowania u sprawcy świadomości wysokiego stopnia prawdopodobieństwa rozpowszechniania nielegalnie utrwalonego lub zwielokrotnionego programu komputerowego przez inną osobę fizyczną lub prawną, która to świadomość nie wywołuje u sprawcy działań zmierzających do przeciwdziałania takiemu rozpowszechnianiu lub rezygnacji z czynności zmierzających do utrwalenia lub zwielokrotnienia programu komputerowego. Dodać wypada, że koniecznym elementem podmiotowym jest brak u sprawcy czynu zabronionego z art. 117 ustawy o prawie autorskim i prawach pokrewnych przeświadczenia, że do rozpowszechniania programu nie dojdzie.[286] Podmiot, który nie godzi się na rozpowszechnianie utrwalonego lub zwielokrotnionego przez siebie utworu nie realizuje znamion przestępstwa z art. 117 prawa autorskiego,[287] nawet jeżeli utrwalił lub zwielokrotnił utwór działając w celu osiągnięcia korzyści majątkowej. W takim wypadku realizuje natomiast znamiona kradzieży programu komputerowego z art. 278 § 2 k.k. W kontekście przedstawionych wyżej uwag można stwierdzić, iż ze względu na zawarty w znamionach przestępstwa piractwa komputerowego wymóg co najmniej godzenia się sprawcy na rozpowszechnianie bezprawnie uzyskanego poprzez zwielokrotnienie lub utrwalenie programu komputerowego, który nie występuje w znamionach przestępstwa określonego w art. 278 § 2 k.k., między zachowaniami opisanymi w obu analizowanych typach czynu zabronionego zachodzi istotna różnica w stopniu bezprawia. Z uwagi na konieczność obejmowania przez sprawcę zwielokrotnienia lub utrwalenia programu komputerowego co najmniej zamiarem wynikowym czynności polegających na rozpowszechnianiu tak uzyskanego programu kom-

[285] Nazwą tą posługuje się A. Adamski, *Przestępstwa komputerowe...*, s. 120. Zob. też M. Byrska, *Prawnokarna ochrona programów komputerowych w nowym prawie autorskim* (w:) *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, red. A. Adamski, Toruń 1994, s. 216 i n.

[286] Por. Z. Ćwiąkalski (w:) *Komentarz do ustawy o prawie autorskim...*, s. 488.

[287] *Ibidem*.

puterowego, można stwierdzić, że stopień bezprawia zachowań stypizowanych w art. 117 ustawy o prawie autorskim i prawach pokrewnych jest większy niż stopień bezprawia zachowań opisanych w art. 278 § 2 k.k.[288] Artykuł 117 prawa autorskiego stanowi więc *lex specialis* w stosunku do art. 278 § 2 k.k. Kłopot związany z wzajemną relacją omawianych przepisów polega jednak na tym, że typ kwalifikowany określony w art. 117 ust. 2 przewiduje niższą sankcję niż przewidziana w typie podstawowym z art. 278 § 2 k.k. W przypadku wielokrotnego uzyskania (przyjmującego postać jego zwielokrotnienia lub utrwalenia) programu komputerowego bez uprawnienia oraz co najmniej godzenia się sprawcy na rozpowszechnianie uzyskanych egzemplarzy (art. 117 ust. 2 prawa autorskiego), będzie on podlegał łagodniejszej sankcji niż w przypadku jednorazowej kradzieży programu komputerowego z art. 278 § 2 k.k. Mamy więc w tym przypadku do czynienia z ewidentną niekoherencją systemu. W piśmiennictwie zaprezentowano rozwiązanie tego dylematu poprzez uznanie, iż w przypadku art. 278 § 2 k.k. i art. 117 ust. 1 i 2 ustawy o prawie autorskim i prawach pokrewnych mamy do czynienia z „częściową derogacją milczącą przepisu art. 117 ust. 1 i 2 ustawy o prawie autorskim i prawach pokrewnych przez przepis art. 278 § 2 k.k. (*lex posterior derogat legi priori*)".[289] Rozwiązanie to wywołuje jednak zasadnicze wątpliwości i wymaga głębszej analizy w kontekście teoretycznego statusu reguł derogacyjnych. Z uwagi na charakter opracowania nie może ona zostać tutaj podjęta, warto jednak podkreślić, że niezwykle trudno jest wskazać teoretyczne uzasadnienie dla koncepcji „milczącej derogacji" w sytuacji, gdy poświęcona zagadnieniom derogacyjnym ustawa z dnia 20 marca 1997 r. — Przepisy wprowadzające Kodeks karny przyjmuje w art. 3 generalną regułę uchylenia wszystkich przepisów dotyczących „przedmiotów unormowanych w Kodeksie karnym, chyba że przepisy tej ustawy stanowią inaczej", i jednocześnie w art. 5 § 1 pkt 33 oraz art. 5 § 2 pkt 36 i 37 stanowi, że pozostawia się w mocy przepisy art. 115, 116, 117, 118 i 120–122 ustawy o prawie autorskim i prawach pokrewnych, dokonując w nich kosmetycznej jedynie zmiany w sferze kolejności kar przewidzianych za te przestępstwa. W kontekście przytoczonych unormowań Przepisów wprowadzających Kodeks karny, wola ustawodawcy co do pozostawienia w mocy przepisów karnych ustawy o prawie autorskim i prawach pokrewnych jest całkowicie czytelna i jednoznaczna, co wyklucza możliwość uznania, iż przepisy te lub co najmniej część z nich

[288] Pogląd taki prezentują także E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 217 i A. Adamski, *Przestępstwa komputerowe...*, s. 120–121.

[289] Koncepcję tę przedstawił A. Adamski, *Przestępstwa komputerowe...*, s. 121.

ulegają derogacji na mocy jednej z dyrektyw interpretacyjnych. W tym stanie rzeczy należy wskazać, iż najlepszym wyjściem byłaby odpowiednia interwencja ustawodawcy, ustawiająca prawidłowo wzajemne relacje tych unormowań.[290]

PASERSTWO PROGRAMU KOMPUTEROWEGO — ART. 293 § 1 K.K. W ZW. Z ART. 291 LUB ART. 292 K.K.

16. Kodeks karny z 1997 r., wprowadzając szczególny typ przestępstwa kradzieży w postaci kradzieży programu komputerowego, zawiera także odpowiednią szczegółową regulację problematyki paserstwa programu komputerowego. Zgodnie z brzmieniem art. 293 § 1 k.k., „przepisy art. 291 i 292 stosuje się odpowiednio do programu komputerowego". Wykorzystana w art. 293 technika legislacyjna jest rzadko spotykana w ustawodawstwie karnym.[291] Konstrukcja art. 293 § 1 k.k. oparta jest na podwójnym odesłaniu. Z jednej strony, przepis ten odwołuje się do treści art. 291 i 292 k.k., określających przestępstwa umyślnego i nieumyślnego paserstwa, z drugiej zaś — zawiera zasadę odpowiedniego stosowania normatywnej charakterystyki obu typów czynu zabronionego do programu komputerowego. Przynajmniej częściowe wyjaśnienie zastosowanej przez ustawodawcę w art. 293 § 1 k.k. techniki legislacyjnej tkwi w charakterze przedmiotu ochrony paserstwa przewidzianego w tym przepisie. Określone w art. 291 i 292 k.k. odmiany paserstwa umyślnego i nieumyślnego charakteryzują czynność wykonawczą jako nabycie, przyjęcie, pomoc do zbycia lub ukrycia rzeczy uzyskanej za pomocą czynu zabronionego. Z uwagi na wykładnię pojęcia „rzecz", nawiązującą jednoznacznie do cywilistycznego rozumienia tego terminu, nie obejmuje ono swym zakresem treściowym programu komputerowego. Program komputerowy, nie będąc rzeczą, tym samym nie może stanowić przedmiotu przestępstwa paserstwa.[292] Aby uniknąć bezkarności paserstwa, którego przedmiotem jest program komputerowy uzyskany za pomocą czynu zabronionego, ustawodawca wprowadził odrębny typ paserstwa odnoszący się do tego przedmio-

[290] Postulat przeprowadzenia nowelizacji przepisów ustawy o prawie autorskim i prawach pokrewnych zgłosiła już wcześniej E. Czarny–Drożdżejko (*Ochrona informacji...*, s. 217).

[291] A. Adamski określa przepis art. 293 jako „oryginalną i nie mającą odpowiedników w prawie porównawczym konstrukcją prawną" (*Przestępstwa komputerowe...*, s. 122).

[292] Por. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 217–218; B. Michalski, *Przestępstwa przeciwko mieniu...*, s. 281.

tu.[293] Artykuł 293 § 1 k.k. nie opisuje samodzielnie znamion przestępstwa paserstwa programu komputerowego, lecz zawiera odesłanie do treści art. 291 k.k. (charakteryzującego typ paserstwa umyślnego) oraz do treści art. 292 k.k. (charakteryzującego typ paserstwa nieumyślnego). Opis typu czynu zabronionego paserstwa programu komputerowego ma zatem w każdym przypadku charakter złożony, jest bowiem wyrażany przez dwa przepisy: w odniesieniu do paserstwa umyślnego typu podstawowego przez art. 293 § 1 w zw. z art. 291 § 1 k.k., w odniesieniu do paserstwa umyślnego typu uprzywilejowanego przez art. 293 § 1 w zw. z art. 291 § 2 k.k., w odniesieniu do paserstwa nieumyślnego w typie podstawowym przez art. 293 § 1 w zw. z art. 292 § 1 k.k. oraz w odniesieniu do paserstwa nieumyślnego typu kwalifikowanego przez art. 293 § 1 w zw. z art. 292 § 2 k.k.

Artykuł 293 § 1 k.k. zawiera klauzulę odpowiedniego stosowania obu wymienionych w nim przepisów do programu komputerowego. Pojęcie odpowiedniego stosowania przepisów nie jest jednoznacznie rozumiane w piśmiennictwie oraz orzecznictwie. W opracowaniach teoretycznych wskazuje się, że odpowiednie stosowanie przepisów oznaczać może, w zależności od kontekstu normatywnego, trzy rodzaje zastosowania przepisu, do którego odnosi się klauzula odpowiedniego stosowania. Pierwszy polega na zastosowaniu danego przepisu wprost, bez dokonywania w nim jakichkolwiek zmian lub dostosowań. Drugi rodzaj polega na zastosowaniu przepisu objętego klauzulą, z jednoczesnym dokonaniem w nim modyfikacji dostosowujących go do przedmiotu regulacji, który określony jest w przepisie zawierającym klauzulę odpowiedniego stosowania. Trzeci rodzaj sprowadza się do orzeczenia niemożności zastosowania przepisu objętego klauzulą odpowiedniego stosowania.[294] Poszukując odpowiedzi na pytanie, który z przedstawionych wyżej sposobów odpowiedniego stosowania przepisów znajdzie zastosowanie w przypadku klauzuli wyrażonej w art. 293 § 1 k.k., warto przyjrzeć się bliżej charakterystyce zachowań podlegających kryminalizacji na podstawie przepisów, do których odnosi się klauzula odpowiedniego stosowania, oraz charakterystyce zachowania, do którego prawnej oceny mają być one odpowiednio stosowane. Między zachowaniem sprawcy dopuszczającego się czynów zabronionych opisanych w art. 291 i 292 k.k. oraz zachowaniem, które charakteryzować mają łącznie art. 293 § 1 w zw. z art. 291 lub w zw. z art. 292 k.k., zachodzi jedna tylko istotna różnica. W przypadku zachowań odpowiadających opisowi zawartemu w art. 291 lub 292, przedmiotem paserstwa jest „rzecz pochodząca z czynu zabronionego", zaś w przypadku zachowania określonego w art. 293 § 1 w zw. z art. 291 lub 292 k.k. — nie będący rzeczą program komputerowy. Z istoty przedmiotu paserstwa z art. 293 § 1 w zw. z art. 291 lub 292 k.k. wynika, iż dopuszczenie się w stosunku do niego charakterystycznych dla paserstwa czynności co do zasady nie będzie wymagało przenoszenia posiadania przedmiotu materialnego, lecz ograniczać się będzie do udostępnienia programu komputerowego sprawcy, który, jak zgrabnie ujmuje to E. Czarny–Drożdżejko, na przykład „nie nabędzie przedmiotu materialnego, lecz specyficzny wytwór ludzkiego intelektu".[295] W pozostałym zakresie zachowania charakteryzujące paserstwo w przypadku rzeczy ruchomej oraz programu komputerowego są wręcz identyczne. Między charakterystyką zachowań karalnych na podstawie art. 291, art. 292 i 293 § 1 w zw. z art. 291 lub 292 k.k. zachodzi daleko idąca zbieżność w charakterystyce zachowania sprawcy. Przesądza to, moim zdaniem, o wykorzystaniu drugiego z przedstawionych wyżej teoretycznych modeli odpowiedniego stosowania przepisów art. 291 i 292 k.k., polegającego na wykorzystaniu powołanych przepisów z odpowiednimi modyfikacjami. Modyfikacja przybierać będzie w tym przypadku postać tzw. prostej zmiany, polegającej na zastąpieniu pojęcia „rzecz", które występuje w art. 291 i 292 k.k. i stanowi jednocześnie przedmiot paserstwa, terminem „program komputerowy", zaczerpniętym z treści art. 293 § 1 k.k. W pozostałym zakresie paserstwo programu komputerowego charakteryzować się będzie tymi samymi elementami normatywnymi, które określają zwykłe odmiany paserstwa.[296]

Niezależnie od oryginalnego sposobu charakterystyki znamion czynu zabronionego, polegającego na zastosowaniu klauzuli odpowiedniego stosowania innych przepisów, przyjęty w Kodeksie karnym sposób regulacji przestępstwa paserstwa programu komputerowego budzi pewne wątpliwości związane z relacją tej odmiany paserstwa do przepisów art. 294 i 295 k.k. Poważne wątpliwości wywołuje bowiem kwestia możliwości stosowania do paserstwa komputerowego przepisów art. 294 i art. 295 k.k.

Ustawowa regulacja paserstwa wyrażona w art. 293 § 1 stanowi, iż do paserstwa programu komputerowego znajdują odpowiednie zastosowanie regulacje zawarte w art. 291 i 292 k.k. Jednocześnie na mocy wyraźnych postanowień zawartych w art. 294 i 295 oba te przepisy znajdują zastosowanie do paserstwa umyślnego (art. 291) oraz nieumyślnego (art. 292). Artykuł 294

[293] Zob. M. Dąbrowska–Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 307.

[294] Co do przypadków odpowiedniego stosowania przepisów — zob. szerzej Z. Siwik, *Systematyczny komentarz do ustawy karnej skarbowej. Część ogólna*, Wrocław 1993, s. 58.

[295] E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 218.

[296] Por. M. Dąbrowska–Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 308–309.

k.k. stanowi w § 1, że „Kto dopuszcza się przestępstwa określonego w art. 278 § 1 lub 2, art. 284 § 1 lub 2, art. 285 § 1, art. 286 § 1, art. 287 § 1, art. 288 § 1 lub 3, lub w art. 291 § 1, w stosunku do mienia znacznej wartości, podlega karze pozbawienia wolności od roku do lat 10". Wedle § 2 tego przepisu natomiast, „Tej samej karze podlega sprawca, który dopuszcza się przestępstwa wymienionego w § 1 w stosunku do dobra o szczególnym znaczeniu dla kultury". Natomiast art. 295 k.k., określający podstawy nadzwyczajnego złagodzenia kary lub odstąpienia od jej wymiaru stanowi w § 1: „Wobec sprawcy przestępstwa określonego w art. 278, 284–289, 291, 292 lub 294, który dobrowolnie naprawił szkodę w całości albo zwrócił pojazd lub rzecz mającą szczególne znaczenie dla kultury w stanie nieuszkodzonym, sąd może zastosować nadzwyczajne złagodzenie kary, a nawet odstąpić od jej wymierzenia". Wedle § 2 tego przepisu, „Wobec sprawcy przestępstwa wymienionego w § 1, który dobrowolnie naprawił szkodę w znacznej części, sąd może zastosować nadzwyczajne złagodzenie kary". W obu przytoczonych wyżej przepisach wśród przestępstw, do których znajdują one zastosowanie nie został wymieniony ani sam art. 293 k.k., ani ten przepis powiązany odpowiednio z przepisami art. 291 i 292 k.k. Na płaszczyźnie wykładni językowej należy zatem stwierdzić, że przepisy art. 294 i 295 k.k., nie wymieniając w katalogu przestępstw, do których znajdują zastosowanie przestępstwa paserstwa komputerowego, tym samym nie odnoszą się do tego typu czynu zabronionego. Teza ta znajduje dodatkowe wsparcie w treści samego art. 293 § 1 k.k., który wyraźnie stanowi, że do programu komputerowego stosuje się odpowiednio przepisy art. 291 i 292, całkowicie pomijając regulacje zawarte w art. 294 i 295 k.k.

W związku z przyjętym sposobem uregulowania odpowiedzialności za paserstwo programu komputerowego należy stwierdzić, że ustawa określa zasady odpowiedzialności za: umyślne paserstwo programu komputerowego typu podstawowego (art. 293 § 1 w zw. z art. 291 § 1 k.k.); umyślne paserstwo programu komputerowego typu uprzywilejowanego (art. 293 § 1 w zw. z art. 291 § 2 k.k.); nieumyślne paserstwo programu komputerowego typu podstawowego (art. 293 § 1 w zw. z art. 292 § 1 k.k.) oraz nieumyślne paserstwo typu kwalifikowanego (art. 293 § 1 w zw. z art. 292 § 2 k.k.). Kodeks karny nie zawiera natomiast żadnych postanowień dotyczących umyślnego paserstwa programu komputerowego przedstawiającego znaczną wartość (tzn. odpowiadającą równowartości przewidzianej w Kodeksie karnym dla mienia znacznej wartości — art. 115 § 5 k.k.) oraz umyślnego paserstwa programu komputerowego stanowiącego dobro o szczególnym znaczeniu dla

kultury. Istnieje natomiast w kodeksie szczególna regulacja odnosząca się do typu kwalifikowanego nieumyślnego paserstwa programu komputerowego (art. 293 § 1 w zw. z art. 292 § 2 k.k.), przy czym znamieniem kwalifikującym jest dopuszczenie się paserstwa w stosunku do programu komputerowego o znacznej wartości. W odniesieniu do typów kwalifikowanych paserstwa programu komputerowego mamy więc do czynienia w Kodeksie karnym z ewidentną antynomią. Z jednej bowiem strony ustawodawca wyraźnie reguluje zagadnienie odpowiedzialności za kwalifikowany typ nieumyślnego paserstwa z uwagi na znaczną wartość przedmiotu przestępstwa (programu komputerowego), z drugiej zaś — nie wypowiada się w ogóle co do odpowiedzialności za dopuszczenie się umyślnego paserstwa w stosunku do przedmiotu o znacznej wartości (programu komputerowego). W sferze odpowiedzialności za umyślne paserstwo programu komputerowego znacznej wartości występuje więc w Kodeksie karnym swoista luka prawna. W tym stanie rzeczy możliwe są dwa teoretyczne rozwiązania. Pierwsze polega na konstatacji tego faktu normatywnego i opiera odpowiedzialność w każdym przypadku umyślnego paserstwa programu komputerowego na konstrukcji typu podstawowego określonego w art. 293 § 1 w zw. z art. 291 § 1 k.k. Koncepcja ta nie prowadzi do braku odpowiedzialności za tę postać paserstwa, z tym jednak, iż w takim wypadku granice ustawowego zagrożenia przewidziane za umyślne paserstwo programu komputerowego znacznej wartości, kwalifikowane na podstawie art. 293 § 1 w zw. z art. 291 § 1 k.k., są identyczne jak zagrożenia przewidziane za nieumyślne paserstwo programu komputerowego znacznej wartości, kwalifikowane na podstawie art. 293 § 1 w zw. z art. 292 § 2 k.k. W konsekwencji, przy zastosowaniu tego rozwiązania dochodzi do zatarcia odmienności między dwoma zachowaniami istotnie różniącymi się między sobą stopniem bezprawia, co prawidłowo oddaje ustawodawca w regulacjach dotyczących umyślnego paserstwa rzeczy znacznej wartości, określonych w art. 291 § 1 w zw. z art. 294 § 1 k.k. (zagrożenie karą pozbawienia wolności od roku do lat 10) oraz nieumyślnego paserstwa rzeczy znacznej wartości w art. 292 § 2 k.k. (zagrożenie karą pozbawienia wolności od 3 miesięcy do lat 5). Drugie z możliwych rozwiązań sprowadza się do podjęcia próby poszukiwania sposobu wypełnienia próżni normatywnej w sferze odpowiedzialności za umyślne paserstwo programu komputerowego znacznej wartości poprzez wykorzystywane w prawoznawstwie metody wypełniania luk. Podstawową metodą wypełniania luk w ustawie jest stosowanie tzw. analogii, a zwłaszcza analogii *legis*. Metoda ta polega na zastosowaniu do wypadku nieprzewidzianego wprost w przepisach prawa przepisu regulu-

jącego zasady odpowiedzialności za przypadki najbardziej doń zbliżone.[297] Próbując zastosować tę metodę do omawianego przypadku, warto rozpocząć rozważania od analizy treści art. 294 § 1 k.k. Opisuje on zbiorczo dla dziesięciu typów przestępstw typ kwalifikowany, w którym okolicznością uzasadniającą surowszą odpowiedzialność jest dopuszczenie się przez sprawcę wymienionych w nim przestępstw w stosunku do mienia znacznej wartości. W przepisie tym wymieniony został typ czynu zabronionego określony w art. 291 § 1 k.k. Tym samym powiązanie ze sobą przepisów art. 291 § 1 i art. 294 § 1 k.k. prowadzi do odczytania znamion charakteryzujących kwalifikowany typ umyślnego paserstwa, który różni się od typu podstawowego znamieniem określającym przedmiot czynności wykonawczej. W typie kwalifikowanym zostaje określona minimalna wartość przedmiotu czynności wykonawczej, która w chwili czynu powinna przekraczać dwustukrotną wysokość najniższego miesięcznego wynagrodzenia. Z tak wyznaczoną wartością przedmiotu czynności wykonawczej powiązana jest nowa granica ustawowego zagrożenia, która ulega podwyższeniu w dolnym progu z 3 miesięcy do 1 roku, zaś w górnym progu z 5 do 10 lat pozbawienia wolności. Artykuł 294 § 1 k.k. wraz z art. 291 § 1 k.k. określa więc znamiona typu kwalifikowanego. Z tego względu do tego przepisu stosują się wprost określone w Konstytucji RP (art. 42 ust. 1) oraz w części ogólnej Kodeksu karnego podstawowe zasady odpowiedzialności karnej. W kontekście prowadzonych rozważań szczególnego znaczenia nabiera, wynikająca m.in. z treści art. 42 ust. 1 Konstytucji RP oraz z art. 1 § 1 k.k., reguła *nullum crimen sine lege*. Rozwinięciem tej reguły jest m.in. zakaz stosowania w prawie karnym analogii, której wynik stanowiłby podstawę pociągnięcia jednostki do odpowiedzialności karnej za czyn, który albo w ogóle nie realizuje wprost znamion typu czynu zabronionego, albo zagrożony jest surowszą karą aniżeli przestępstwo, którego znamiona czyn sprawcy wprost realizuje.[298] Zgodnie z zasadą *nullum crimen sine lege certa*, podstawą odpowiedzialności karnej może być tylko zgodność czynu sprawcy ze znamionami typu czynu zabronionego określonymi w ustawie karnej. Dla odpowiedzialności karnej w żadnym wypadku nie jest wystarcza-

[297] Zob. J. Nowacki, *Analogia legis*, Warszawa 1966, s. 9 i n.; W. Świda, *Prawo karne*, Warszawa 1986, s. 84; W. Wolter, *Prawo karne. Zarys wykładu systematycznego. Część ogólna*, Warszawa 1947, s. 22; A. Zoll (w:) *Kodeks karny. Część ogólna...*, s. 34 i n.

[298] Zob. A. Zoll (w:) *Kodeks karny. Część ogólna...*, s. 34–35; R. Dębski, *Pozaustawowe znamiona przestępstwa. O ustawowym charakterze norm prawa karnego i znamionach typu czynu zabronionego nie określonych w ustawie*, Łódź 1995, s. 12 i n.; L. Gardocki, *Zasada nullum crimen sine lege a akty normatywne naczelnych organów administracji*, Państwo i Prawo 1969, nr 9, s. 519 i n.; T. Bojarski, *Typizacja przestępstw i zasada nullum crimen sine lege (wybrane zagadnienia)*, Annales UMCS 1977, t. XXIV, s. 147 i n.

jące podobieństwo poddawanego ocenie zachowania do czynów realizujących znamiona określonego typu czynu zabronionego.[299] Odnosząc przedstawione wyżej reguły do przypadku popełnienia umyślnego paserstwa programu komputerowego znacznej wartości stwierdzić należy, iż w rzeczywistości zachowania polegające na nabywaniu, przyjmowaniu, pomaganiu w zbyciu lub pomaganiu w ukryciu programu komputerowego uzyskanego za pomocą czynu zabronionego (art. 293 § 1 w zw. z art. 291 § 1) są bardzo zbliżone do zachowań wypełniających znamiona przestępstwa umyślnego paserstwa rzeczy określonego w art. 291 § 1 k.k. Oba te zachowania różnią się normatywnie dwoma elementami: określeniem przedmiotu czynności wykonawczej oraz formalną podstawą kwalifikacji. W przypadku zwykłego paserstwa — powtórzmy to raz jeszcze — przedmiotem czynności wykonawczej jest rzecz, zaś podstawą kwalifikacji jest art. 291 § 1 k.k. W przypadku paserstwa programu komputerowego przedmiotem czynności wykonawczej jest właśnie taki program, zaś podstawą kwalifikacji — art. 293 § 1 w zw. z art. 291 § 1 k.k. Obie te różnice mają istotne znacznie dla odpowiedzialności karnej. Ukazują bowiem, że umyślne paserstwo oraz umyślne paserstwo programu komputerowego to dwa różne typy czynu zabronionego, różniące się formalnie (tzn. przepisami zawierającymi znamiona tych przestępstw) oraz merytorycznie (tzn. treścią tych znamion). W odniesieniu do paserstwa rzeczy znacznej wartości, k.k. z 1997 r. zawiera wyraźną i jednoznaczną regulację, stwarzającą podstawy do zbudowania z dwóch jednostek tekstu prawnego, tj. z art. 291 § 1 i art. 294 § 1 k.k., znamion paserstwa typu kwalifikowanego ze względu na wartość przedmiotu. W odniesieniu do paserstwa programu komputerowego znacznej wartości, k.k. z 1997 r. nie zawiera żadnej regulacji. Stanowiący podstawę odpowiedzialności za paserstwo programu komputerowego art. 293 § 1 k.k. nie zawiera żadnego odniesienia do art. 294 § 1 k.k., podobnie art. 294 § 1 k.k. nie wymienia wśród przepisów, do których ma on zastosowanie, art. 293 § 1. Oznacza to, że Kodeks karny nie zawiera żadnej reguły nakazującej stosowanie przepisu art. 294 § 1 do paserstwa programu komputerowego. Nie istnieją więc na gruncie tej ustawy podstawy do zbudowania typu kwalifikowanego paserstwa programu komputerowego ze względu na wartość programu. Odpowiedzialność za kwalifikowany typ umyślnego paserstwa (art. 294 § 1 w zw. z art. 291 § 1 k.k.), w przypadku gdy jego przedmiotem jest program komputerowy o znacznej wartości, musiałaby więc opierać się na analogii na niekorzyść sprawcy, która w obszarze prawa karnego

[299] Zob. szerzej w tej kwestii R. Dębski, *Pozaustawowe znamiona przestępstwa...*, s. 19 i n. oraz cytowana tam literatura, zwłaszcza pochodząca z niemieckiego obszaru językowego.

jest niedopuszczalna. Tym samym należy stwierdzić, iż niezależnie od wartości programu komputerowego, w każdym przypadku umyślnego paserstwa podstawą odpowiedzialności karnej jest typ określony w art. 293 § 1 w zw. z art. 291 § 1 k.k.[300] Aktualnie obowiązujący Kodeks karny nie określa bowiem kwalifikowanego typu umyślnego paserstwa programu komputerowego ze względu na wartość programu.[301] Identycznie rozstrzygać należy zagadnienie paserstwa programu komputerowego o szczególnym znaczeniu dla kultury.

Ostatnim zagadnieniem wywołującym wątpliwości interpretacyjne jest wzajemny stosunek zawartych w Kodeksie karnym z 1997 r. przepisów statuujących poszczególne odmiany paserstwa programu komputerowego do przepisu art. 118 ustawy o prawie autorskim i prawach pokrewnych, regulującego zagadnienie paserstwa nośnika utworu. Zgodnie z brzmieniem art. 118 ust. 1 ustawy o prawie autorskim i prawach pokrewnych, „Kto w celu osiągnięcia korzyści majątkowej przedmiot będący nośnikiem utworu, artystycznego wykonania, fonogramu, wideogramu rozpowszechnianego lub zwielokrotnianego bez uprawnienia lub wbrew jego warunkom nabywa, pomaga w jego zbyciu, przyjmuje albo pomaga w jego ukryciu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Wedle art. 118 ust. 2, „Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności do lat 3". Przepis art. 118 ustawy o prawie autorskim i prawach pokrewnych oraz przepisy k.k. z 1997 r. odnoszące się do paserstwa programu komputerowego wykazują daleko idące podobieństwo. Z jednej strony, identycznie określają znamiona czynności wykonawczej, z drugiej, mają identycznie określony przedmiot, albowiem utworem jest także program komputerowy. W obu przypadkach mamy ewidentnie do czynienia z podstawą karalności paserstwa. Poza tym generalnym podobieństwem, odnaleźć można kilka istotnych różnic między wskazanymi przepisami. Pierwsza z nich odnosi się do określenia strony podmiotowej, która w przypadku paserstwa programu komputerowego przewidzianego w k.k. przybierać może postać zarówno umyślności (w obu odmianach),

[300] Zob. szerzej M. Dąbrowska-Kardas, P. Kardas, *Przestępstwa przeciwko mieniu...*, s. 309–312.

[301] Odmienne stanowisko w tej kwestii zajmuje B. Michalski, stwierdzając, że „dla szczególnych odmian paserstwa określonych w art. 293 § 1, zarówno umyślnego, jak i nieumyślnego — przewidziano w k.k. z 1997 r. odmiany kwalifikowane ze względu na znaczną wartość będącego ich przedmiotem mienia (tj. programu komputerowego), gdyż odmiany takich przestępstw kwalifikowanych przewidziano odpowiednio dla paserstwa unormowanego w art. 291 (w art. 294 § 10, a dla paserstwa nieumyślnego w art. 292 § 2)" (*Przestępstwa przeciwko mieniu...*, s. 282).

jak i nieumyślności, zaś w przypadku art. 118 ustawy o prawie autorskim i prawach pokrewnych ograniczona jest do umyślności, przy czym ustawa wymaga ponadto, aby sprawca działał w celu osiągnięcia korzyści majątkowej.[302] Druga różnica dotyczy przedmiotu czynności wykonawczej, którym na gruncie przepisów k.k. z 1997 r. dotyczących paserstwa może być każdy program komputerowy uzyskany za pomocą czynu zabronionego, natomiast na gruncie art. 118 ustawy o prawie autorskim i prawach — jedynie nośnik programu komputerowego, który jest rozpowszechniany lub zwielokrotniany bez uprawnienia albo wbrew jego warunkom.[303] Oba te elementy sprawiają, że czyny zabronione określone w art. 118 ustawy o prawie autorskim i prawach pokrewnych mają znacznie węższy zakres zastosowania niż czyny zabronione określające różne odmiany paserstwa programu komputerowego, znajdujące się w Kodeksie karnym.[304] Ponadto charakterystyka zachowania karalnego opisanego w art. 118 ustawy o prawie autorskim wskazuje na znacznie większy stopień bezprawia niż charakterystyka zachowań opisanych w odmianach paserstwa programu komputerowego w k.k. z 1997 r. O większym bezprawiu czynu z art. 118 ustawy o prawie autorskim przesądzają: konieczna na gruncie tego typu umyślność zachowania sprawcy, uzupełniona koniecznością działania w celu osiągnięcia korzyści majątkowej, oraz warunek rozpowszechniania lub zwielokrotniania programu komputerowego przed dokonaniem czynności sprawczej paserstwa.[305] Wszystkie wymienione wyżej okoliczności zdają się sugerować, że między przepisami regulującymi zasady odpowiedzialności za paserstwa programu komputerowego, znajdującymi się w Kodeksie karnym, a przepisem art. 118 ustawy o prawie autorskim i prawach pokrewnych zachodzi stosunek specjalności, przy czym art. 118 jest przepisem szczególnym.[306] Takiej relacji między porównywanymi przepisami sprzeciwia się natomiast zestawienie sankcji przewidzianych za analizowane przestępstwa, które na gruncie art. 118 prawa autorskiego są znacznie niższe niż w art. 293 § 1 w zw. z art. 291 § 1 k.k. W przypadku paserstwa występuje więc podobna niekoherencja systemowa jak w omówionym powyżej w niniejszym opracowaniu przypadku kradzieży programu komputerowego. Podobnie jak w odniesieniu do kradzieży programu komputerowego, usunięcie tej antynomii nie jest możliwe poprzez odwołanie się do konstrukcji częścio-

[302] Zob. Z. Ćwiąkalski (w:) *Komentarz do ustawy o prawie autorskim...*, s. 490.

[303] Zob. *ibidem*, s. 490 i n.; A. Adamski, *Przestępstwa komputerowe...*, s. 123.

[304] Por. A. Adamski, *Przestępstwa komputerowe...*, s. 123.

[305] Zob. E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 220.

[306] *Ibidem*.

wej milczącej derogacji.[307] Jedynym sposobem rozwiązania istniejącej sytuacji jest nowelizacja przepisów ustawy o prawie autorskim i prawach pokrewnych i dostosowanie ich do rozwiązań przyjętych w Kodeksie karnym z 1997 r. Przygotowywana nowelizacja prawa autorskiego z całą pewnością stwarza ku temu bardzo dobrą okazję.[308]

[307] Koncepcję taką prezentuje A. Adamski, *Przestępstwa komputerowe...*, s. 124.

[308] Przeprowadzenie koniecznych zmian dostosowawczych do Kodeksu karnego w ustawie o prawie autorskim i prawach pokrewnych postuluje także E. Czarny–Drożdżejko, *Ochrona informacji...*, s. 221.

CZASOPISMO PRAWA KARNEGO I NAUK PENALNYCH
Rok IV: 2000, z. 1 ISSN 1506–1817

WŁODZIMIERZ WRÓBEL

PRAWNOKARNA OCHRONA TAJEMNICY PAŃSTWOWEJ

1. WSTĘP

Zmiany zachodzące we współczesnej kulturze coraz dobitniej uzasadniają przekonanie, iż kolejne stulecie stanie się cywilizacją społeczeństwa informatycznego.[1] Już obecnie informacja traktowana jest nie tylko jako intratny przedmiot obrotu gospodarczego, ale także jako instrument gwarantujący zachowanie władzy politycznej i militarnej oraz dający możliwość sprawowania kontroli społecznej. Skomplikowane procesy przetwarzania informacji ogarniają coraz szersze dziedziny życia społecznego, a od ich prawidłowego przebiegu zależy bezpieczeństwo i normalne funkcjonowanie ogromnych rzesz ludzi.

Problematyka prawa do informacji oraz ochrony informacji stała się nader pilnym zagadnieniem legislacyjnym ostatnich lat, zwłaszcza w kontekście pojawiających się wraz z rozwojem informatyki zagrożeń, których najjaskrawszym objawem jest przestępczość komputerowa oraz naruszenia praw własności intelektualnej

Konieczność weryfikacji dotychczasowych instrumentów prawnej ochrony informacji nie mogła ominąć tajemnicy państwowej. Zmiany legislacyjne, jakie w tym zakresie nastąpiły Polsce w ostatnich latach, uwarunkowane były nie tylko wskazanymi wcześniej przemianami kulturowymi, ale wynikały także z radykalnej transformacji ustroju politycznego państwa. Postulat dostosowania ustawodawstwa do wymogów demokratycznego państwa prawa po

[1] Por. A. Lekka–Lowalik, *Demokracja i autonomia jednostki w globalnej strukturze informacyjnej* (w:) *Zagrożenia etyczne wynikające z rozwoju informatyki*, Nauka 1999, nr 1, s. 125 i n., tamże: W. Wróbel, *Społeczeństwo informatyczne — szanse i zagrożenia*, s. 159 i n.