Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego t. XVI, 18 (2) 2021, s. 7-23
https://doi.org/10.32084/sawp.2021.16.2-1

Michał Czakowski

PRZESTĘPSTWA PRZECIWKO OCHRONIE INFORMACJI. WYBRANE ZAGADNIENIA PRAWNO-MATERIALNE I KRYMINOLOGICZNE

Wprowadzenie

Bezpieczeństwo każdego państwa związane jest z zapewnieniem ograniczenia dostępu do pewnych informacji istotnych dla jego funkcjonowania. Dlatego też tworzone są systemy ochrony informacji, które nie są powszechnie jawne [Chałubińska-Jentkiewicz 2017, 578-79]. Informacje niejawne to takie, „których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależne od formy i sposobu jej wyrażania”[1].

Część I

We współczesnym świecie informacja towarzyszy człowiekowi na każdym etapie jego aktywności, czy to o charakterze zawodowym, bądź też w wymiarze prywatnym. K. Chałubińska-Jentkiewicz wskazuje, iż „informacja jest składnikiem wartości, które mają zasadnicze znaczenie dla różnych organizacji [...] prywatnych i państwowych” [tamże, 576]. Informacja podlega przetwarzaniu oraz utrwalaniu w różnorodnych formach, począwszy od formy ustnej, pisemnej w tradycyjnym wymiarze, po formę z zastosowaniem środków elektronicznych. Bez względu na okoliczność i sposób

Dr Michał Czakowski, Wydział Nauk Prawnych, Społecznych i Humanistycznych, Kujawsko-Pomorska Szkoła Wyższa w Bydgoszczy; adres do korespondencji: ul. Toruńska 55-57, 85-023 Bydgoszcz, Polska; e-mail: m.czakowski@kpsw.edu.pl; https://orcid.org/0000-0001-7463-3490

[1] Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*, Dz. U. z 2019 r., poz. 742 z późn. zm. [dalej: u.o.i.n.].

jej przetwarzania, informacja powinna być zawsze dostatecznie chroniona, „zwłaszcza jeśli udostępnianie związane jest z sytuacjami o charakterze szczególnie istotnym dla państwa" [tamże]. Do nadrzędnych celów państwa zaliczyć należy zatem zapewnienie należytej ochrony informacji, tj. bezpieczeństwa informacji, bowiem od tego zależy jego „sprawne i bezpieczne funkcjonowanie" [tamże, 577]. W polskim systemie prawa pojęcie „informacji" niejawnych, zgodnie z art. 1 ust. 1 u.o.i.n. dotyczy informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo z punktu widzenia jej interesów byłoby niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania. Ustawodawca w przepisie art. 5 u.o.i.n. dokonał klasyfikacji informacji niejawnych, określając jednocześnie zasady i warunki nadawania im określonego rodzaju klauzul: *ściśle tajne*, *tajne*, które stanowią przedmiot penalizowanych w *Kodeksie karnym*[2] przestępstw, a także *poufne* i *zastrzeżone* (art. 5 ust. 3 i 4 u.o.i.n.). Klauzule *ściśle tajne* oraz *tajne* nadawane są tym informacjom niejawnym, których ujawnienie spowodowałoby „poważną" lub „wyjątkowo poważną" szkodę dla kraju [Chałubińska-Jentkiewicz 2017, 594]. Znaczenie przestrzegania zasad i procedur przewidzianych przez ustawodawcę w przepisach ustawy *o ochronie informacji niejawnych* ma istotny wpływ na bezpieczeństwo państwa. Stąd ustawodawca zdecydował o konieczności wprowadzenia mechanizmów oraz systemu egzekwowania konsekwencji działań niepożądanych wymierzonych w państwo i obywateli podejmowanych przez podmioty w zakresie informacji niejawnych.

Postępowaniu w sprawie informacji niejawnych poświęcony jest także art. 225 *Kodeksu postępowania karnego*[3]. Wskazany przepis stanowi, że wydane lub znalezione przy przeszukaniu pismo lub inny dokument zawierający informacje niejawne lub wiadomości objęte tajemnicą zawodową czy inną tajemnicą prawnie chronioną albo ma charakter osobisty, organ przeprowadzający czynność przekazuje niezwłocznie, bez jego odczytania prokuratorowi lub sądowi w opieczętowanym opakowaniu. Odpowiedzialność

[2] Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny*, Dz. U. z 2021 r., poz. 1023 z późn. zm. [dalej: k.k.].

[3] Ustawa z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego*, Dz. U. z 2018 r., poz. 1987 z późn. zm.

karna jest „jednym z rodzajów odpowiedzialności, która dotyczy sfery przetwarzania informacji i przy tym konieczności zapewnienia im ochrony" [Chałubińska-Jentkiewicz 2017, 594]. Organy oraz funkcjonariusze publiczni, a także inne wskazane podmioty ponoszą odpowiedzialność na podstawie przepisów rozdziału XXXIII k.k. zatytułowanego „Przestępstwa przeciwko ochronie informacji" (art. 265-269c k.k.). Przyjąć należy za K. Chałubińską-Jentkiewicz, iż „penalizacji podlega nie tylko zabronione działanie w stosunku do samej informacji, ale również nielegalna ingerencja w system lub sieć, w ramach których informacja funkcjonuje. W literaturze przedmiotu wskazuje się, iż jako przedmiotem ochrony tegoż rozdziału k.k. uznać należy informację, jako „jedno z najbardziej dynamicznie zmieniających się dóbr prawnych" [Chałubińska-Jentkiewicz 2017, 594; Hałas 2019; Hoc 2019]. Przestępstwa penalizowane w rozdziale XXXIII k.k. ująć można w cztery grupy [Hałas 2019; Hoc 2019]. Do pierwszej grupy zalicza się przepisy chroniące informację będącą tajemnicą, zaś do drugiej grupy – przepisy chroniące informację przed zniszczeniem lub naruszeniem albo brakiem dostępu do niej, bądź też zakłócaniem automatycznego przetwarzania danych informatycznych. Trzecią grupę przepisów rozdziału XXXIII k.k. stanowią przepisy chroniące urządzenia techniczne służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych, natomiast czwartą grupę – przepisy chroniące wytwarzanie, w tym czynności do tego zbliżone, urządzeń lub programów komputerowych przystosowanych do popełnienia określonych przestępstw, haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub w sieci teleinformatycznej. Pojęcie „informacji" w ujęciu przepisów k.k. należy rozumieć jako „wiadomość lub sumę wiadomości o osobie albo o stanie rzeczy, dotyczącą faktów, stanowiącą logiczną całość" [Hałas 2019]. W zależności od charakteru informacji i kręgu podmiotów, której ona dotyczy, może być uznana za dobro prywatne lub też ponadindywidualne [tamże]. Przestępstwo penalizowane w art. 265 § 1 k.k. polega na ujawnieniu lub wbrew przepisom ustawy wykorzystaniu informacji niejawnych o klauzuli „tajne" lub „ściśle tajne"[4]. W ocenie A. Sakowicza nie stanowi dokonania przestępstwa sam fakt ujawnienia informacji

[4] Warto w tym miejscu wskazać na rozumienie pojęcia.

z określonych przez ustawodawcę kategorii [Sakowicz 2017, 8]. Dokonanie przestępstwa ma miejsce wówczas, gdy sens tej informacji zostanie zrozumiany [tamże]. Istotną kwestią jest także rozumienie pojęcia „ujawnienie". Pojęcie ujawnienia jest szerokie. W ocenie S. Hoca „ujawnieniem jest to, co nazywamy zdradą tajemnicy, wyjawieniem tajemnicy, udzieleniem komuś wiadomości stanowiącej tajemnicę, zakomunikowaniem wiadomości, jej rozpowszechnianiem, rozgłoszeniem, udostępnieniem komuś, opublikowaniem itp." [Hoc 2019]. Autor słusznie zwraca uwagę, iż „w pojęciu ujawnienia mieszczą się różne sposoby działania sprawcy, takie jak wypowiedź ustna, udostępnienie pisma zawierającego tajemnicę, okazanie dokumentu lub przedmiotu (choćby bez wydania go z rąk) itp., zamieszczone w środkach przekazu (np. telefon, faks), ujawnienie [...] przy użyciu komputera, np. przez nadanie jej pocztą elektroniczną, przy wykorzystaniu Internetu" [tamże]. Uważa się także, że „w poprawnej polszczyźnie ujawnienie oznacza czynienie jawnym tego, co dotąd jawne nie było" [tamże]. Nazwę tę utożsamia się także z „ujawnieniem tajemnicy".

Karą pozbawienia wolności od 3 miesięcy do 5 lat, zgodnie z art. 265 § 1 k.k., zagrożony jest czyn polegający na ujawnieniu lub wbrew przepisom ustawy wykorzystaniu informacji niejawnych o klauzuli „tajne" lub „ściśle tajne". Jeśli sprawca ujawnił tę informację osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, podlega karze pozbawienia wolności od 6 miesięcy do lat 8 (art. 265 § 2 k.k.). Typ nieumyślny czynu zabronionego, o którym stanowi przepis art. 265 § 1 k.k., ustawodawca określił w § 3 stanowiąc, że kto nieumyślnie ujawnia informację państwową, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 podlega ten, kto wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, na mocy przepisu art. 266 § 1 k.k. Z kolei ujawnienie przez funkcjonariusza publicznego osobie nieuprawnionej informacji niejawnej o klauzuli „zastrzeżone" lub „poufne" lub informacji, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes,

podlega karze pozbawienia wolności do lat 3 (art. 266 § 2 k.k.). Podmiotem przestępstwa w tym przypadku może być jedynie funkcjonariusz publiczny, tym samym sprawca musi być funkcjonariuszem publicznym zarówno w czasie ujawnienia informacji, jak i w momencie zapoznawania się z rzeczoną informacją [Hoc 2019; Chałubińska-Jentkiewicz 2017, 595].

Kolejnym z przestępstw penalizowanych przez ustawodawcę w przepisach rozdziału XXXIII k.k. jest nielegalne uzyskanie informacji. Naruszenie tajemnicy korespondencji, to czyn zabroniony uregulowany w art. 267 § 1 k.k. Polega on na uzyskaniu bez uprawnienia dostępu do informacji, która nie jest przeznaczona dla sprawcy, przez otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia informacji. Karany jest także czyn polegający na uzyskiwaniu bez uprawnienia dostępu do całości lub części systemu informatycznego (art. 267 § 1 k.k.), zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem w celu uzyskania informacji, do której sprawca nie jest uprawniony (§ 3), jak również ujawnianie innej osobie informacji uzyskanych w warunkach tego przestępstwa [Hałas 2019].

Dla transparentności i bezpieczeństwa procesu wyborczego, a w szczególności zapewnienia bezpieczeństwa informacji w jego toku, niezwykle istotna jest okoliczność penalizacji czynów zabronionych, które mogą wówczas zaistnieć. Ustawodawca w k.k. dokonał także klasyfikacji i penalizacji następujących czynów zabronionych: niszczenia informacji (art. 268 k.k.), dokonania szkody w bazach danych (art. 268a k.k.), sabotażu komputerowego (art. 269 k.k.), zakłócenia pracy w sieci (art. 269a k.k.), bezprawnego wykorzystania programów i danych (art. 269b k.k.).

Czyn zabroniony, jakim jest niszczenie, uszkadzanie, usuwanie lub dokonywanie zmian zapisu istotnej informacji przez osobę nieuprawnioną, bądź udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznania się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 268 § 1 k.k.). Wymiar kary pozbawienia wolności jest wyższy – do 3 lat, w odniesieniu do tego samego czynu zabronionego, lecz dotyczącego zapisu na informatycznym nośniku danych (art. 268 § 2 k.k.). Jeżeli w związku z popełnieniem tychże czynów

wystąpiła szkoda majątkowa, zgodnie z § 3 czyny te podlegają wyłącznie karze pozbawienia wolności od 3 miesięcy do 5 lat. Uzasadnieniem dla wprowadzenia przez ustawodawcę kar dla tego rodzaju czynu zabronionego było, jak słusznie wskazuje S. Hoc, „[...] rosnące znaczenia informacji dla prawidłowego funkcjonowania różnych dziedzin życia oraz poważne, negatywne następstwo zakłócenia systemu gromadzenia i wykorzystywania informacji, szczególnie w zakresie odgrywającej coraz ważniejszą rolę informacji komputerowej" [Hoc 2019].

Poprzez ujęcie dwóch zbiorczych zachowań sprawcy w art. 268a k.k. – przedmiotem pierwszego jest niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych albo w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych przez osoby nieuprawnione, przedmiotem drugiego ujęcia jest natomiast zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych w istotnym stopniu przez osoby nieuprawnione. Oba czyny podlegają karze pozbawienia wolności do lat 3.

Przestępstwo określone w art. 269 § 1 k.k. polega na niszczeniu, uszkodzeniu lub zmianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego [tamże]. Ujęcie dalsze tego czynu zabronionego odnosi się do przekazywania danych wymienionych w tym przepisie. Przestępstwo określone w art. 269 § 2 k.k. polega na popełnieniu czynu określonego w § 1 przez niszczenie lub wymianę informatycznego nośnika danych, albo niszczenie lub uszkodzenie urządzenia służącego do automatycznego przetwarzania, gromadzenia bądź przekazywania danych informatycznych [tamże]. Istotą sabotażu komputerowego jest „wprowadzenie, modyfikacja, wymazanie lub zablokowanie danych lub programów komputerowych albo inne oddziaływanie na system komputerowy mające na celu wywołanie zakłóceń w funkcjonowaniu systemu komputerowego lub telekomunikacyjnego" [Kunicka-Michalska 2018, 1036]. Nadrzędnym przedmiotem ochrony w popełnianych tego rodzaju przestępstwach jest „obronność kraju, bezpieczeństwo w komunikacji, funkcjonowanie administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego" [tamże, 1037].

Karą pozbawienia wolności od 3 miesięcy do lat 5 zagrożony jest czyn polegający na transmitowaniu, zniszczeniu, usunięciu, uszkodzeniu, utrudnianiu dostępu lub zmianie danych informatycznych, w istotny sposób zakłócając tym samym pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej (art. 269a k.k.). Jest to jedna z postaci sabotażu komputerowego [tamże, 1042]. Przez pojęcie „transmisji" należy rozumieć „przekazywanie na odległość dźwięku i obrazu" [Hałas 2019].

Natomiast w przepisie art. 269b k.k. ustawodawca penalizuje przestępstwo dysponowania i obrotu tzw. narzędziami hakerskimi [tamże]. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2, art. 269 § 1 lub 2, albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Choć ustawodawca nie wyeksplikował tego faktu, to nie ulega wątpliwości, iż dobrem podlegającym ochronie są zarówno prywatne, jak i publiczne systemy informatyczne i teleinformatyczne oraz sieci teleinformatyczne, a nade wszystko bezpieczeństwo informacji.

Część II

Szczegółowe statystyki dotyczące przestępstw przeciwko ochronie informacji w okresie od 1999 r. do 2019 r. prezentowane są na stronach policji:

Tabela 1: Ujawnienie tajemnicy państwowej (art. 265)

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2019	2	0
2018	3	0
2017	1	1
2016	2	2
2015	2	4
2014	2	3
2013	5	4
2012	12	10
2011	14	9
2010	16	12
2009	16	3
2008	12	5
2007	14	4
2006	9	6
2005	6	11
2004	4	10
2003	0	5
2002	0	9
2001	1	9
2000	2	6
1999	1	12

Źródło: https://statystyka.policja.pl/download/20/361941/Ujawnienietajemnicypanstwowej-art265xslx.xlsx [dostęp: 30.04.2021].

Analizując dane zaprezentowane w tabeli 1, w szczególności te najnowsze, obserwuje się, iż liczba przestępstw począwszy od 2013 r. utrzymuje się na niewysokim poziomie, a w 2019 r. nie stwierdzono żadnego naruszenia.

Interesującym jest fakt, iż niewspółmiernie dużą liczbę wszczętych postępowań zarejestrowano w przedziale od 2007 r. do 2014 r.

Tabela 2: Ujawnienie tajemnicy służbowej i zawodowej (art. 266)

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2019	174	53
2018	164	53
2017	163	62
2016	139	218
2015	147	49
2014	127	33
2013	148	50
2012	159	77
2011	131	47
2010	162	59
2009	155	82
2008	121	50
2007	133	42
2006	159	85
2005	131	121
2004	125	58
2003	99	50
2002	94	54
2001	75	48
2000	82	27
1999	43	32

Źródło: https://statystyka.policja.pl/download/20/361942/Ujawnienietajemnicysluzbowejizawodowej-art266.xlsx [dostęp: 30.04.2021].

Analiza przedstawionego zestawienia z tabeli 2 pozwala stwierdzić, iż liczba wszczynanych postępowań związanych z naruszeniem tajemnicy zawodowej i służbowej w kontekście od 1999 r. aż do 2019 r.

poza nielicznymi wyjątkami ma tendencję wzrostową. W 2016 r. rekordowo stwierdzono 218 przestępstw.

Tabela 3: Naruszenie tajemnicy korespondencji (art. 267)

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2019	6 718	5 196
2018	3 676	2 597
2017	3 419	2 503
2016	3 401	2 718
2015	3 515	2 452
2014	2 868	1 901
2013	2 203	1 655
2012	1 657	1 513
2011	1 583	948
2010	1 194	1 102
2009	982	645
2008	694	505
2007	616	384
2006	538	370
2005	430	260
2004	378	248
2003	362	232
2002	294	215
2001	259	175
2000	249	240
1999	182	113

Źródło: https://statystyka.policja.pl/download/20/361943/Naruszenietajemnicykorespondencji-art267.xlsx [dostęp: 30.04.2021].

Informacje zawarte w tabeli 3, wskazują, że na przestrzeni lat 1999-2019, liczba postępowań wszczętych dotyczących naruszenia tajemnicy korespondencji wzrastała, poza nielicznymi wyjątkami, osiągając w 2019 r.

rekordowe 6718 wszczętych postępowań. Jednocześnie w tym samym roku stwierdzono 5196 przestępstw.

Tabela 4: Udaremnienie lub utrudnienie korzystania z informacji (art. 268 i 268a)

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2019	868	642
2018	530	2 432
2017	654	703
2016	712	789
2015	759	579
2014	743	572
2013	765	589
2012	796	884
2011	885	629
2010	690	479
2009	555	1 115
2008	366	249
2007	244	168
2006	201	136
2005	152	98
2004	105	89
2003	114	138
2002	89	167
2001	60	118
2000	66	48
1999	59	49

Źródło: https://statystyka.policja.pl/download/20/361944/Udaremnienielubutrudnieniekorzystaniazinformacji-art268i268a.xlsx [dostęp: 30.04.2021].

W oparciu o statystyki zaprezentowane w tabeli 4, analizując dane, w szczególności te najnowsze, można zauważyć, iż liczba przestępstw stwierdzonych związanych z udaremnieniem lub utrudnieniem korzystania z informacji osiągnęła maksimum 2432 w 2018 r. Liczba

postępowań wszczynanych począwszy od 2010 r. aż do 2019 r. utrzymywała się na względnie podobnym poziomie.

Tabela 5: Niszczenie danych informatycznych (art. 269)

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2019	17	9
2018	9	6
2017	13	3
2016	11	6
2015	4	4
2014	10	6
2013	14	9
2012	9	5
2011	3	5
2010	7	0
2009	6	2
2008	6	2
2007	6	0
2006	3	4
2005	2	3
2004	12	0
2003	2	2
2002	6	12
2001	9	5
2000	7	5
1999	10	3

Źródło: https://statystyka.policja.pl/download/20/361945/Niszczeniedanychinformatycznych-art269.xlsx [dostęp: 30.04.2021].

Dane prezentowane w tabeli 5, w szczególności te najnowsze, pozwalają wysnuć wniosek, iż liczba przestępstw związanych z niszczeniem danych informatycznych jest potencjalnie nie duża, chociaż w 2002 r. stwierdzono rekordowo 12 takich przestępstw. Natomiast w 2019 r. wszczęto najwięcej bo 17 postępowań dotyczących tego typu naruszeń.

Tabela 6: Sabotaż komputerowy (art. 269a)

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2019	37	34
2018	51	41
2017	39	34
2016	44	38
2015	52	38
2014	27	48
2013	37	34
2012	35	30
2011	38	30
2010	22	18
2009	34	243
2008	13	13
2007	11	11
2006	19	19
2005	1	1

Źródło: https://statystyka.policja.pl/download/20/361946/Sabotazkomputerowy-art269a.xlsx [dostęp: 30.04.2021].

Liczba przestępstw wszczętych w związku z sabotażem komputerowym, czyli naruszeniem art. 269a k.k., w oparciu o informacje wskazane w tabeli 6, była największa w 2015 r. i wyniosła 52. Natomiast w 2009 r. stwierdzono aż 243 takich przestępstw.

Tabela 7: Wytwarzanie programu komputerowego do popełnienia przestępstwa (art. 269b)

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2019	55	39
2018	29	34
2017	28	24
2016	36	39
2015	58	44
2014	47	43
2013	42	28
2012	21	27
2011	38	29
2010	35	71
2009	23	18
2008	12	12
2007	4	4
2006	9	9
2005	6	6

Źródło: https://statystyka.policja.pl/download/20/361947/Wytwarzanieprogramukomputerowegodopopelnieniaprzestepstwa-art269b.xlsx [dostęp: 30.04.2021].

Analiza danych z tabeli 7 pozwala stwierdzić, iż liczba wszczętych postępowań związanych z wytwarzaniem programu komputerowego do popełnienia przestępstwa (art. 269b) była największa w 2015 r. i wyniosła 58, jednocześnie w tym samym roku stwierdzono popełnienie przestępstwa w 44 przypadkach.

Zakończenie

Zważywszy na interpretacje przepisów, wszelkie informacje, które mają nadaną odpowiednią klauzulę zgodnie z ustawą *o ochronie informacji niejawnych* muszą być w odpowiedni sposób chronione z zachowaniem trybu i sposobu przewidzianego przez nią. Natomiast dokumenty, dane dla których przewidziano ochronę w oparciu o przepisy ogólne, nie dotyczące

informacji niejawnych będą zabezpieczane w oparciu o konkretne regulacje prawne wskazane dla danego przypadku. Wprowadzony przez ustawodawcę, a następnie konsekwentnie uzupełniany i modyfikowany na przestrzeni kilkunastu lat katalog przestępstw przeciw ochronie, ale także bezpieczeństwu informacji, stanowi jedno z wielu działań państwa zmierzających do zapewnienia szeroko pojętego jego bezpieczeństwa [Ciekanowski 2019, 193]. Współcześnie działalność sprawcza w tej kategorii przestępstw na coraz większą skalę przenosi się z przestrzeni realnej, do przestrzeni wirtualnej, tj. cyberprzestrzeni [Fischer 2000, 25n.].

PIŚMIENNICTWO

Chałubińska-Jentkiewicz, Katarzyna. 2017. „Ochrona danych osobowych a powszechny obowiązek obrony Rzeczpospolitej Polskiej." W *Prawo wojskowe*, red. Waldemar Kitler, Dariusz Nowak, i Marta Stepanowska, 578-95. Warszawa: Wolters Kluwer Polska.

Ciekanowski, Zbigniew. 2019. „Bezpieczeństwo państwa w cyberprzestrzeni." W *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki – organizacji – państwa*, red. Sylwia Wojciechowska-Filipek, i Zbigniew Ciekanowski, 187-256. Warszawa: CeDeWu.

Fischer, Bogdan. 2000. *Przestępstwa komputerowe i ochrona informacji*. Kraków: Wolters Kluwer Polska.

Hałas, Radosław. 2019. „Wprowadzenie. Rozdział XXXIII." W *Kodeks karny. Komentarz*, wyd. 6, red. Alicja Grześkowiak, i Krzysztof Wiak. Warszawa: Legalis el.

Hoc, Stanisław. 2019. „Rozdział XXXIII. Przestępstwa przeciwko ochronie informacji." W *Kodeks karny. Komentarz*, wyd. 23, red. Ryszard Stefański. Warszawa: Legalis el.

Kunicka-Michalska, Barbara. 2018. „Przestępstwa przeciwko informacji." W *System Prawa Karnego*. T. 8: *Przestępstwa przeciwko państwu i dobrom zbiorowym*, red. Lech Gadrocki, 1036-42. Warszawa: Wydawnictwo C.H. Beck.

Sakowicz, Andrzej. 2017. „Komentarz do art. 265." W *Kodeks karny. Część szczególna*. Tom 2: *Komentarz do artykułów 222–316*, red. Michał Królikowski, i Robert Zawłocki. Warszawa: Legalis el.

Przestępstwa przeciwko ochronie informacji. Wybrane zagadnienia prawnomaterialne i kryminologiczne

Abstrakt

W XXI w. bezpieczeństwo każdego państwa związane jest z zapewnieniem ograniczenia dostępu do pewnych informacji istotnych dla jego funkcjonowania. Dlatego też tworzone są systemy ochrony informacji. We współczesnym świecie informacja towarzyszy człowiekowi na każdym etapie jego aktywności, czy to o charakterze zawodowym, bądź też w wymiarze prywatnym. Informacja podlega przetwarzaniu oraz utrwalaniu w różnorodnych formach, począwszy od formy ustnej, pisemnej w tradycyjnym wymiarze, po formę z zastosowaniem środków elektronicznych. Do nadrzędnych celów państwa zaliczyć należy zatem zapewnienie należytej ochrony informacji, tj. bezpieczeństwa informacji. W polskim systemie prawa pojęcie informacji niejawnych, zgodnie z art. 1 ust. 1 ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* dotyczy informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo z punktu widzenia jej interesów byłoby niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania. Natomiast organy oraz funkcjonariusze publiczni, a także inne wskazane podmioty ponoszą odpowiedzialność na podstawie przepisów rozdziału XXXIII *Kodeksu karnego* zatytułowanego „Przestępstwa przeciwko ochronie informacji" (art. 265-269c).

Słowa kluczowe: informacja, przestępstwa, bezpieczeństwo informacji

Crimes Against the Protection of Information. Selected Legal and Material Issues and Criminological

Abstract

In the 21st century, the security of each country is related to ensuring that access to certain information essential for its functioning is limited. Therefore, information protection systems are created. In the modern world, information accompanies man at every stage of his activity, be it of a professional or private nature. Information is processed and recorded in various forms, ranging from oral, written in the traditional dimension, to the form using electronic means. Therefore, the overriding objectives of the state include ensuring adequate protection of information, i.e. information security. In the Polish legal system, the concept of classified information, pursuant to Article 1(1) of the Act of 5 August 2010 on the protection of classified information applies to information, the unauthorized disclosure of which would cause or could cause damage to the Republic of Poland or would be unfavorable from the point of view of its interests, also during their development and regardless of the form and manner of their expression.

On the other hand, the authorities and public officials as well as other indicated entities are liable under the provisions of Chapter XXXIII of the Penal Code, entitled "Offenses against the protection of information" (Article 265-269c).

Keywords: information, crimes, information security

Information about Author: Dr. Michał Czakowski, Faculty of Legal, Social and Humanities,, Kujawy and Pomorze University in Bydgoszcz; correspondence address: ul. Toruńska 55-57, 85-023 Bydgoszcz, Poland; e-mail: m.czakowski@kpsw.edu.pl; https://orcid.org/0000-0001-7463-3490