Anna Słowik[1]

OCHRONA DANYCH OSOBOWYCH I PRAWA DO INFORMACJI – KONSEKWENCJE NARUSZENIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Streszczenie: Artykuł zawiera rozważania dotyczące ochrony danych osobowych ujętych w przepisach prawa polskiego i regulacjach międzynarodowych. Porusza kwestię prawa do gromadzenia informacji o obywatelach przez organy władzy publicznej. Zawiera interpretację wyroków Europejskiego Trybunału Praw Człowieka w Strasburgu oraz w szczególności ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, a także dane statystyczne dotyczące wszczętych postępowań i stwierdzonych prawomocnymi wyrokami przestępstw związanych z utrudnianiem organom władzy publicznej dostępu do informacji, niszczeniem danych, sabotażem komputerowym, zapobieganiem wytwarzaniu oprogramowania komputerowego związanego z cyberprzestępczością. W artykule autorka skupia się również na analizie liczby prawomocnych wyroków skazujących orzeczonych przez sądy za tego rodzaju przestępstwa oraz rodzajach kar za nie orzeczonych w ostatnich dwunastu latach.

Słowa kluczowe: ochrona danych osobowych, prawo do informacji, przestępstwa przeciwko ochronie informacji, kary za przestępstwa przeciwko ochronie informacji.

---

[1] dr Anna Słowik, afiliowane: Zakład Zarządzania, Instytut Politechniczny, Państwowa Wyższa Szkoła Zawodowa im. Stanisława Pigonia w Krośnie.

Wstęp

Zakres ochrony danych osobowych został uregulowany ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. Prawo wspólnotowe w tym zakresie reguluje konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 1981 roku, dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 roku w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych[2], a także dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 roku dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej[3]. Dodatkowo istotną rolę w aspekcie ochrony danych osobowych pełni również Generalny Inspektor Ochrony Danych Osobowych – GIODO. Szczegółowe regulacje ujęte są także w przepisach Kodeksu Cywilnego (w szczególności art. 23 i 24).

Źródła ochrony danych osobowych

W ciągu ostatnich lat szczególnie newralgiczną kwestią stało się wykorzystywanie przez poszczególne państwa danych osobowych[4]. Problem ten został dostrzeżony przez Komitet Praw Człowieka ONZ oraz Radę Europy. Ryzyka, jakie rodzi to dla praw jednostki, są powszechnie znane zarówno na szczeblu prawa krajowego, jak i w ramach regulacji międzynarodowych, zwłaszcza w konwencji Rady Europy z 1981 roku o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[5].

Konwencja ta, choć nie została ratyfikowana przez Polskę, tworzy istotny punkt odniesienia dla standardów ustalanych przez Europejską Konwencję Praw

---

[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych, Dz. Urz. WE L 281 z 21.11.1995 r., P. 0031.

[3] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej, Dz. Urz. L 201 z 31.07.2002 r., P. 0037–0047.

[4] Zob. A. Gliszczyńska-Grabias, K. Sękowska-Kozłowska, *Prawo do prywatności*, [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych*, R. Wieruszewski (red.), Warszawa 2011, s. 411.

[5] Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, Strasburg 28 stycznia 1981 r., Dz.U. 2003 nr 3 poz. 25 z późn. zm.

Człowieka[6], której nasz kraj jest stroną. Procedowane są unormowania ograniczające tworzenie zbiorów danych, ich wykorzystywanie w systemie władz publicznych, a także udostępnianie istniejących zbiorów i korygowaniae ich nieprawidłowości. Orzecznictwo strasburskie od dawna zajmuje się tymi kwestiami i – jak w wielu innych dziedzinach – przeszło ewolucję od tolerancyjnego podejścia odnośnie urzędowego gromadzenia danych osobowych do bardziej restrykcyjnego. Państwa zostały zobowiązane do tego, by ograniczyć ingerencję w prywatność obywateli[7] do rzeczywiście „koniecznych" sytuacji[8].

Pewne typy rejestrowania, a więc tworzenia odpowiednich zbiorów danych, nie budzą większych kontrowersji, jednak szczególne problemy wyłoniły się w odniesieniu do zbiorów danych kompilowanych przez służby specjalne i policję. Trybunał nie ma wątpliwości, że „służby specjalne znajdują legitymowane podstawy egzystencji w społeczeństwie demokratycznym", podkreśla jednak zarazem, iż „ich kompetencje do sekretnego śledzenia obywateli są tolerowalne tylko w zakresie ściśle koniecznym dla ochrony demokratycznych instytucji[9]. Istnieje więc uzasadnienie, zwłaszcza gdy w grę wchodzi bezpieczeństwo państwa, dla wydawania ustaw zezwalających służbom specjalnym na „gromadzenie i przechowywanie niejawnych informacji o obywatelach, a także ich wykorzystywanie, np. przy ocenie kwalifikacji osób ubiegających się o zatrudnienie na stanowiskach mających związek z bezpieczeństwem narodowym[10]. Może się to łączyć z przekazywaniem takich informacji innym organom władzy publicznej, zaś zainteresowany może nie być powiadamiany ani o fakcie gromadzenia o nim informacji, ani o zakresie ich przekazywania. Brak takiego powiadamiania zapewnia efektywność stosowanej procedury[11]. Władzom publicznym przysługuje w tych kwestiach „szeroki margines oceny"[12].

---

[6] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności Rzym, 4 listopada 1950 r., zmieniona Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993 nr 61 poz. 284 z późn. zm.

[7] Wyrok ETPCz z 16 lutego 2000 r. w sprawie Amann p. Szwajcarii Recueil des arrêts et décisions, 2000-II, § 65.

[8] Wyrok ETPCz z 6 czerwca 2006 r. w sprawie Segerstedt-Wiberg and Others przeciwko Szwecji, Skarga nr 62332/00.

[9] Tamże, §88.

[10] Wyrok ETPCz z 26 marca 1987 r. w sprawie Leander p. Szwecji, Skarga nr 9248/81, §59.

[11] Tamże.

[12] Wyrok ETPCz w sprawie Segerstedt-Wiberg, §104.

Trybunał dostrzega, iż „istnienie systemu niejawnego gromadzenia informacji służących ochronie bezpieczeństwa państwa tworzy ryzyko podważenia demokratycznego państwa prawnego”[13]. Skłania to Europejski Trybunał Praw Człowieka do coraz bardziej intensywnego formułowania wymagań i gwarancji, koniecznych do realizacji art. 8 EKPCz. Ingerencją w sferę chronioną przez art. 8 jest nie tylko gromadzenie danych o czysto prywatnym charakterze, ale także danych związanych z działalnością publiczną danej osoby. Nie można więc twierdzić, iż podjęcie działalności politycznej kryje w sobie dobrowolną rezygnację z ochrony[14].

W Polsce ochrona danych osobowych wynika z art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej[15] oraz ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych[16].

Prace nad przygotowaniem aktualnej ustawy z 29 sierpnia 1997 roku o ochronie danych osobowych trwały 6 lat. Tworzenie norm prawa z zakresu ochrony danych osobowych należy traktować jako przejaw jurydyzacji obszarów do niedawna „wolnych” od publicznoprawnej ingerencji[17]. Ten stan rzeczy niesie ze sobą interpretacyjne wątpliwości i trudności[18], ale skłania również do obserwowania sposobu stosowania podobnych ustaw w innych krajach, zwłaszcza należących do Unii Europejskiej.

Omawianej ustawie starano się nadać kompleksowy charakter, i to na kilku płaszczyznach. Ustawa reguluje, choć może nazbyt fragmentarycznie, kwestie wolności informacji, czy interes osób trzecich związany z dostępem oraz wykorzystywaniem informacji. Poszukuje w tym zakresie sposobu pogodzenia sprzecznych do pewnego stopnia, interesów. Co przy tym istotne, ustawa nie wprowadza żadnych wyraźnych przepisów, jeśli chodzi o obrót zbiorami (bazami) danych osobowych.

---

[13] Wyrok ETPCz z 22 września 1993 w sprawie Klass, Sygn. 27/1992/372/446, § 49.

[14] Wyrok ETPCz z 4 maja 2000 w sprawie Rotaru, Skarga nr 28341/95, § 43.

[15] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 nr 78 poz. 483 z późn. zm.

[16] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997 nr 133 poz. 883 z późn. zm.

[17] G. Szpor, *Publicznoprawna ochrona danych osobowych*, PUG 1999, nr 12, s. 10.

[18] Skutkujące, z jednej strony, niezrozumieniem czy wręcz lekceważeniem ustawy, z drugiej strony zaś nadgorliwością w jej wdrażaniu i stosowaniu.

Ważną rolę ustawa przyznaje administratorom danych nakładając na nich:

a) rozległe obowiązki informacyjne w stosunku do tych, których zbierane i przetwarzane dane osobowe dotyczą (art. 24–25, art. 32–33, art. 54 u.o.d.o.);
b) obowiązek dbania o legalność i rzetelność przetwarzania danych osobowych (art. 26, art. 49–50 u.o.d.o.);
c) obowiązek dbania o zachowanie danych osobowych w poufności (art. 37–39, art. 51 u.o.d.o.);
d) obowiązek zabezpieczenia zbiorów danych osobowych (art. 36 i n., art. 52 u.o.d.o.);
e) obowiązek rejestracji zbioru (art. 40 i n., art. 53 u.o.d.o.).

Ustawa dotyczy zakresem swego działania zarówno:

a) wszelkich sposobów przetwarzania danych „tradycyjnie" oraz zautomatyzowanie
b) przetwarzania danych w sektorze publicznym i prywatnym[19].

Złożony i kompleksowy charakter ustawy łączy normy przynależne dla różnych dziedzin prawa. Dotyczy to głównie prawa administracyjnego oraz karnego, przy czym dane osobowe chroni się wszystkimi środkami publicznoprawnymi[20]. Należy również zaznaczyć, iż ustawa przyjęła model rejestracyjny w zakresie przetwarzania danych osobowych. W modelu tym przetwarzanie nie jest zależne od uzyskania zezwolenia ze strony władzy, natomiast na administratora danych nałożono obowiązek zgłoszenia zbioru danych Generalnemu Inspektorowi Ochrony Danych Osobowych.

Przetwarzanie danych osobowych dokonywane musi być zgodnie nie tylko z samą ustawą o ochronie danych osobowych, ale także wszystkimi obowiązującymi normami prawa. Jednocześnie zagadnienia ochrony danych osobowych stanowią fragment znacznie szerszego problemu, związanego głównie z „udostępnianiem" ich zawartości. Ustawodawca, uwzględniając praktykę doktryny i judykatury, przewidując być może kierunek zmian technologicznych w stronę popularyzacji komunikacji elektronicznej, określił w tytule ustawy zwrot „ochrona" danych osobowych, nie zaś „przetwarzanie" danych osobowych. Podkreślił on w art. 7 pkt 2 ustawy

---

[19] B. Fischer, *Administrator danych osobowych po przystąpieniu Polski do Unii Europejskiej. Uwagi de lege lata*, „Radca Prawny" 2005, nr 5, s. 94.

[20] Tamże, s. 96.

o ochronie danych osobowych, iż przetwarzanie danych jest operacją zachodząca na danych osobowych głównie w systemach informatycznych[21]. Dane osobowe mogą być przetwarzane w zbiorach danych i poza tym zbiorem (art. 2 ust. 1 i 2 u.o.d.o.). Natomiast „udostępnianie" jest wynikiem przetwarzania danych osobowych i nie zostało zdefiniowane w odrębnych regulacjach.

Konsekwencje naruszenia przepisów o ochronie danych osobowych w instytucjach publicznych

Liczba wszczętych postępowań i popełnionych przestępstw dotyczących niszczenia, uszkadzania, usuwania, zmieniania zapisu, udaremniania lub utrudniania zapoznania się z informacjami organom władzy publicznej (art. 268 k.k. i 268a k.k) w latach 1999–2014 systematycznie wzrastała (zob. rys. 1). Liczba wszczętych postępowań w roku 1999 wyniosła 49, a w roku 2014 już 572. W 2009 roku liczba wszczętych postępowań wzrosła aż do 1115. W roku 1999 wyniosła 59, a w 2014 roku aż 743. Wzrost efektywności w karaniu przestępców popełniających tego rodzaju czyny był możliwy dzięki znacznemu rozwojowi systemów informatycznych umożliwiających lepsze wykrywanie i ściganie osób popełniających przestępstwa przeciwko ochronie informacji.

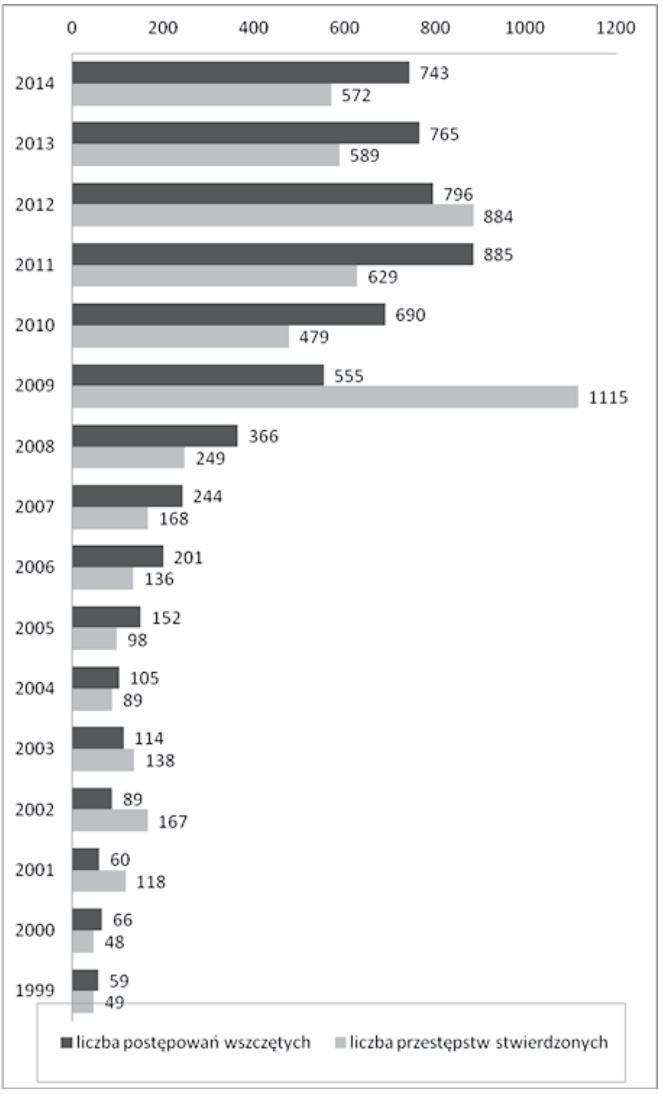
Liczba popełnionych przestępstw i wszczętych postępowań w zakresie niszczenia danych zgodnie z art. 269 k.k. w latach 1999–2014 kształtowała się na poziomie do kilku, kilkunastu rocznie (zob. rys. 2). Jednocześnie w roku 2004, 2007 i 2010 nie stwierdzono przestępstw niszczenia danych.

W zakresie sabotażu komputerowego liczba popełnionych przestępstw i wszczętych na podstawie art. 269a k.k. postępowań od roku 2005 systematycznie wzrastała (zob. rys. 3). W roku 2005 stwierdzono popełnienie tylko jednego przestępstwa i rozpoczęto tylko jedno postępowanie. W latach 2006–2008 liczba ta wyniosła kilkanaście, a od roku 2010 wahała się w przedziale 20–50, przy czym w roku 2009 stwierdzono aż 243 popełnione przestępstwa sabotażu komputerowego. Taki stan rzeczy związany był głównie z wejściem w życie nowelizacji art. 269 a k.k. do którego zakwalifikowano również przestępstwa polegające na utrudnianiu dostępu do danych informatycznych, powodujące zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej.

---

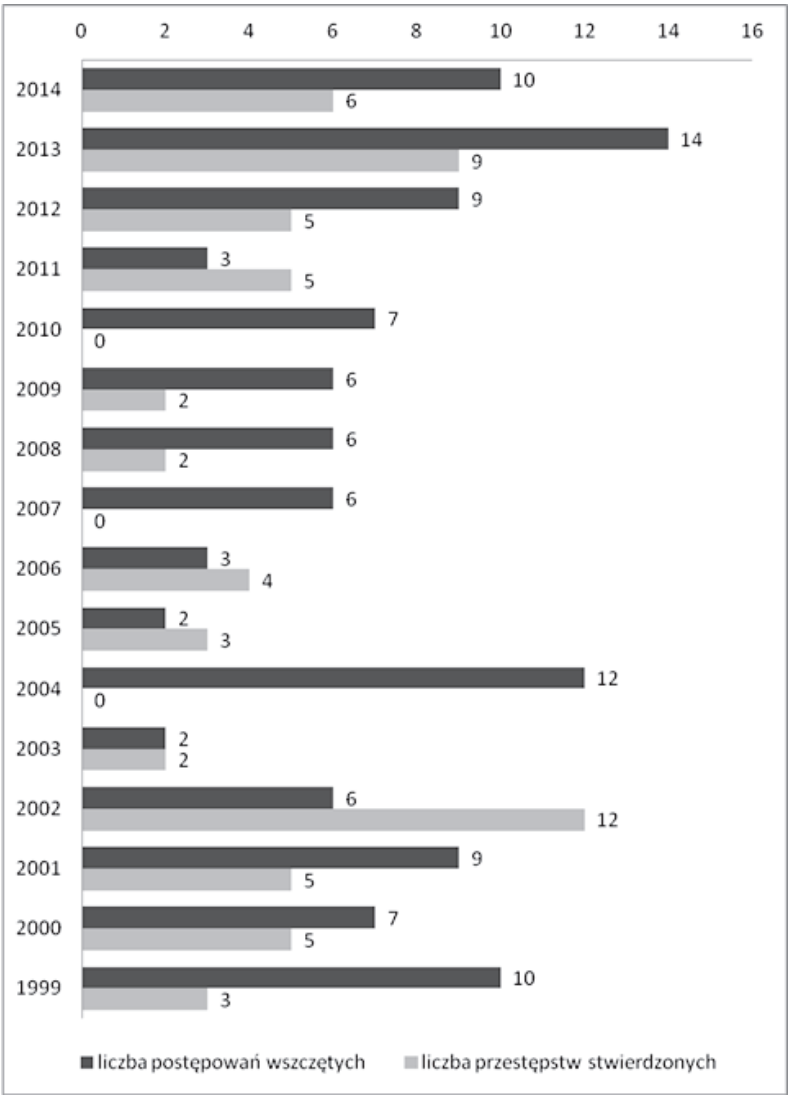
[21] T.R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej*, Warszawa 2004, s. 67.

Rysunek 1. Liczba wszczętych postępowań i popełnionych przestępstw dotyczących niszczenia, uszkadzania, usuwania, zmieniania zapisu, udaremniania lub utrudniania zapoznania się z informacjami organom władzy publicznej (art. 268 k.k. i 268a k.k.)



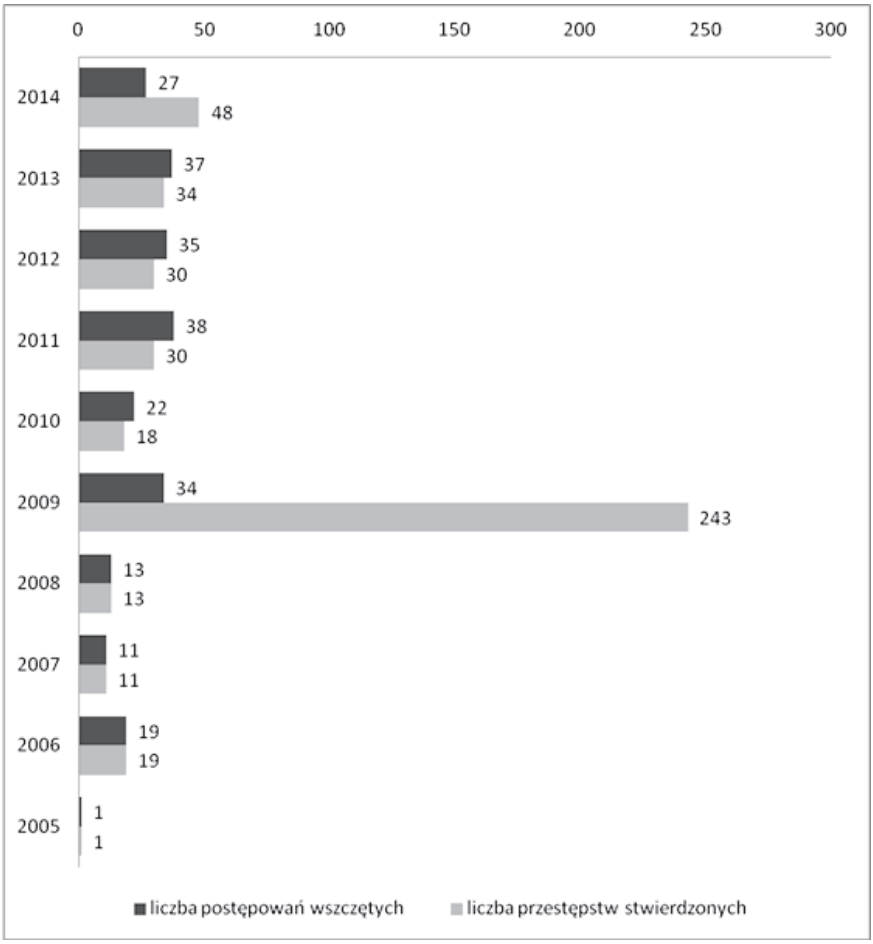
Źródło: *Opracowanie własne na podstawie: http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63626,Udaremnienie-lub-utrudnienie-korzystania-z-informacji-art-268–i-268a.html (dostęp: 18.05.2017)*

Rysunek 2. Liczba popełnionych przestępstw i wszczętych postępowań w zakresie niszczenia danych (art. 269 k.k.)



Źródło: *Opracowanie własne na podstawie: http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63628,Niszczenie-danych-informatycznych-art-269.html (dostęp: 18.05.2017)*

Rysunek 3. Liczba popełnionych przestępstw i wszczętych postępowań w zakresie sabotażu komputerowego (art. 269a k.k.)

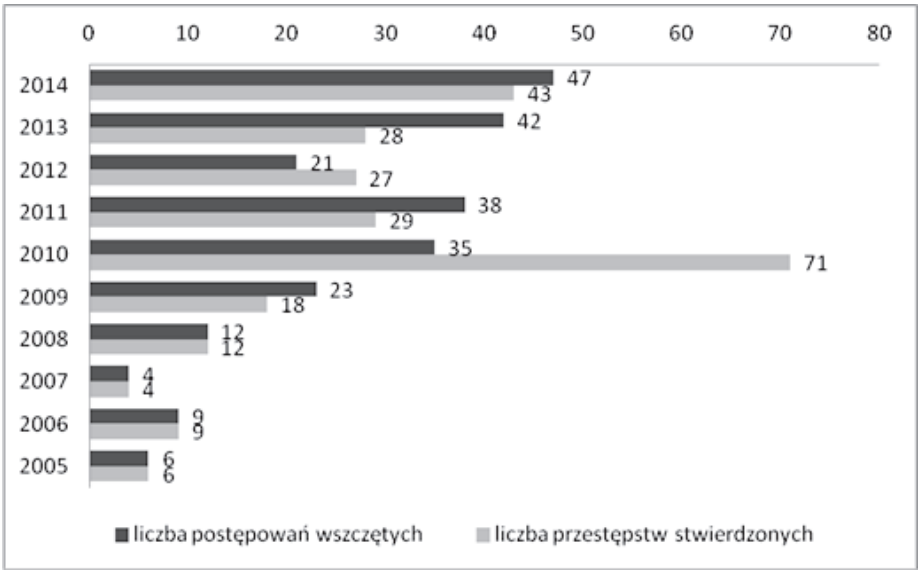


Źródło: *Opracowanie własne na podstawie: http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63630,Sabotaz-komputerowy-art-269a.html (dostęp: 18.05.2017)*

Również liczba popełnionych przestępstw i wszczętych postępowań w zakresie wytwarzania oprogramowania komputerowego służącego do niezgodnego z prawem pozyskiwania informacji (art. 269b k.k.) od roku 2005 systematycznie wzrasta (zob. rys. 4). W roku 2005 odnotowano 6 przestępstw o tym charakterze i wydano 6 postanowień dotyczących wszczęcia postępowania. Natomiast w roku 2014 stwierdzono już 43 naruszenia art. 269b k.k. i wszczęto 47 postępowań.

W roku 2010 stwierdzono rekordową liczbę przestępstw w zakresie wytwarzania oprogramowania komputerowego służącego do niezgodnego z prawem pozyskiwania informacji. Liczba ta wyniosła 71 i była wyższa od łącznej sumy popełnionych przestępstw w latach 2005–2009. Po roku 2010 liczba popełnionych przestępstw już nigdy nie osiągnęła tak wysokiego poziomu. Było to spowodowane nowelizacją art. 269 b k.k. – wskazano bowiem, iż odnosi się on również do sytuacji uwzględnionej w art. 267 § 3 k.k., tj. gdy niezgodne z prawem informacje pozyskiwane są dzięki urządzeniom podsłuchowym, wizualnym lub innym.

Rysunek 4. Liczba popełnionych przestępstw i wszczętych postępowań w zakresie wytwarzania oprogramowania komputerowego służącego do niezgodnego z prawem pozyskiwania informacji (art. 269b k.k.)

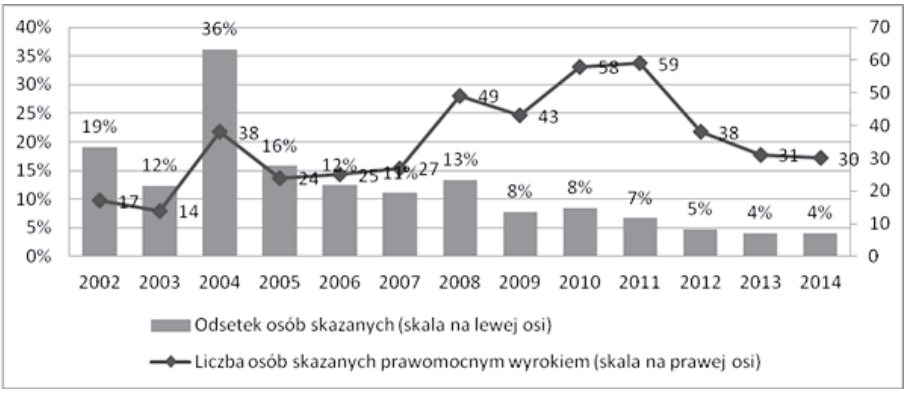


Źródło: *Opracowanie własne na podstawie: http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63633,Wytwarzanie-programu-komputerowego-do-popelnienia-przestepstwa-art-269b.html (dostęp: 18.05.2017)*

W latach 2002–2011 liczba osób skazanych prawomocnym wyrokiem za przestępstwa dotyczące niszczenia, uszkadzania, usuwania, zmieniania zapisu, udaremniania lub utrudniania zapoznania się z informacjami organom władzy publicznej na podstawie art. 268 k.k. i 268a k.k. wzrastała i dopiero po roku 2011

zaczęła spadać (zob. rys. 5). Jednocześnie odsetek osób skazanych za naruszenie norm art. 268 k.k. i 268a k.k. w I instancji, a następnie uniewinnionych systematycznie się obniżał z 19% w roku 2002 do 4% w latach 2013–2014.

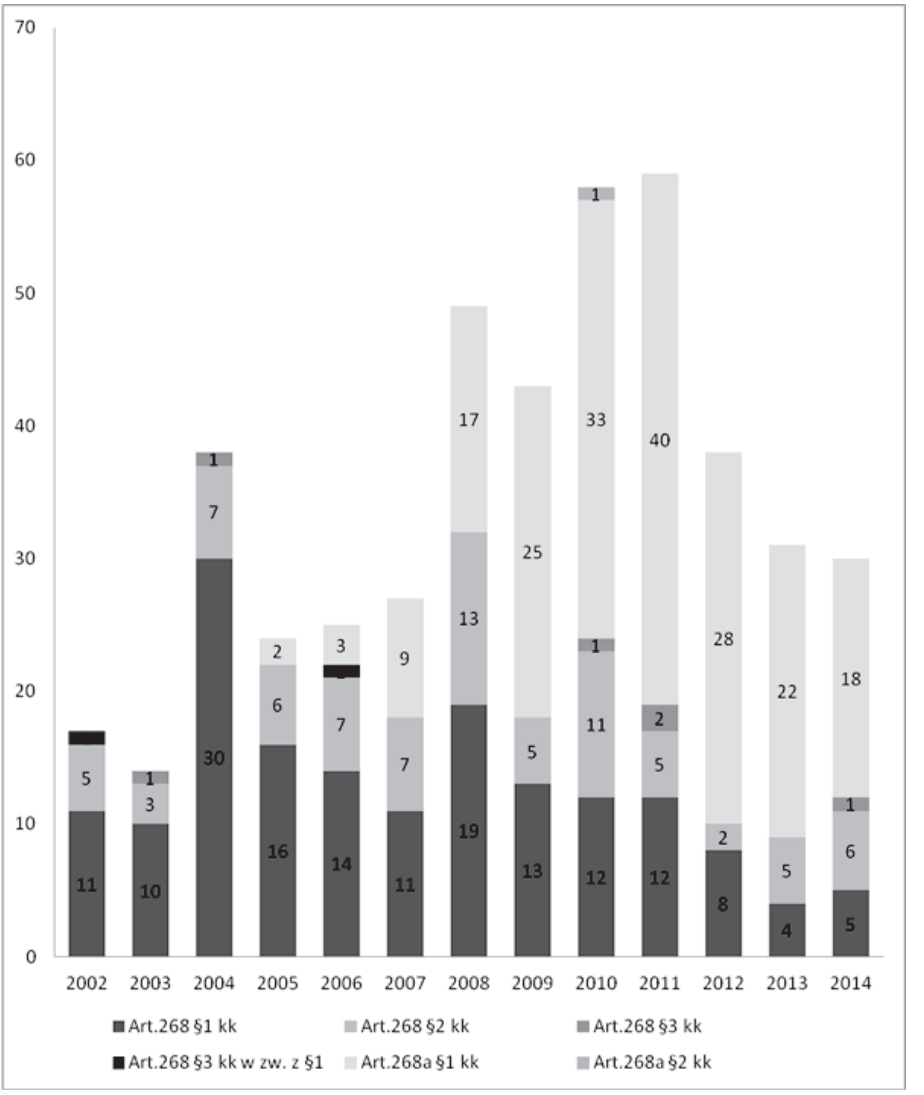
Rysunek 5. Liczba i odsetek osób skazanych za przestępstwa dotyczące niszczenia, uszkadzania, usuwania, zmieniania zapisu, udaremniania lub utrudniania zapoznania się z informacjami organom władzy publicznej (art. 268 k.k. i 268a k.k.)



Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

O ile do roku 2008 największa liczba osób skazywana była za naruszenie art. 268 §1 k.k. (zob. rys. 16), to od roku 2009 najczęściej skazywane są podmioty za naruszenie art. 268a §1 k.k. Wyraźny jest więc wzrost liczby przestępstw polegających na niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu do danych osobowych organom władzy publicznej.

Rysunek 6. Liczba osób skazanych za naruszenie prawa w zakresie niszczenia, uszkadzania, usuwania, zmieniania zapisu, udaremniania lub utrudniania zapoznania się z informacjami organom władzy publicznej (art. 268 k.k. i 268a k.k.)



Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

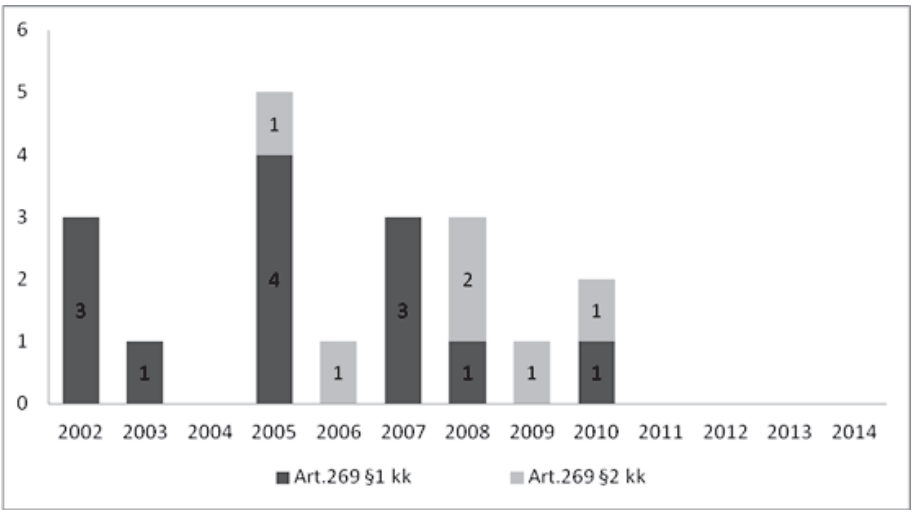
Liczba osób skazanych za niszczenie danych na podstawie art. 269 k.k. w badanym okresie pozostaje bardzo niska, przy czym po roku 2011 nie skazano żadnej osoby na tej podstawie (zob. rys. 7). W latach 2002–2003, 2006 i 2009 odsetek osób skazanych wynosił 50%. W tych latach więc w co drugiej lub co trzeciej sprawie o niszczenie danych informatycznych wydawano wyrok skazujący.

Rysunek 7. Liczba i odsetek osób skazanych za niszczenie danych informatycznych (art. 269 k.k.)

Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

W przypadku liczby osób skazywanych za naruszenie prawa w zakresie niszczenia danych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej do roku 2007 (włącznie) najwięcej osób skazano na podstawie art. 269 §1 (zob. rys. 8), natomiast od roku 2008 przeważała liczba skazanych na podstawie art. 269 §2 k.k..

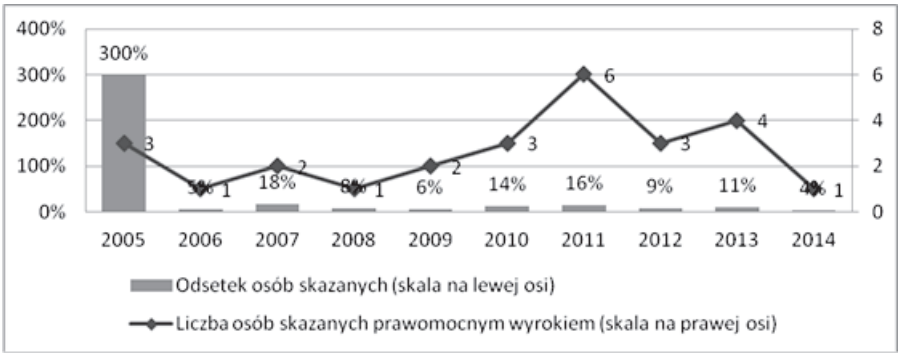
Rysunek 8. Liczba osób skazanych za naruszenie prawa w zakresie niszczenia danych informatycznych (art. 269 k.k.)



Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

W 2005 roku wprowadzono do Kodeksu Karnego nowy typ przestępstwa, które określono w art. 269a k.k. Polega ono na zakłóceniu pracy systemu komputerowego lub sieci komputerowej. Od 2005 do 2011 roku liczba prawomocnych wyroków orzeczonych za popełnienie tego przestępstwa wzrosła (patrz rys. 9). Jednocześnie od roku 2006 odsetek osób skazanych w skali roku za popełnienie przestępstwa z art. 269 a k.k. nie był nigdy wyższy niż 18%.

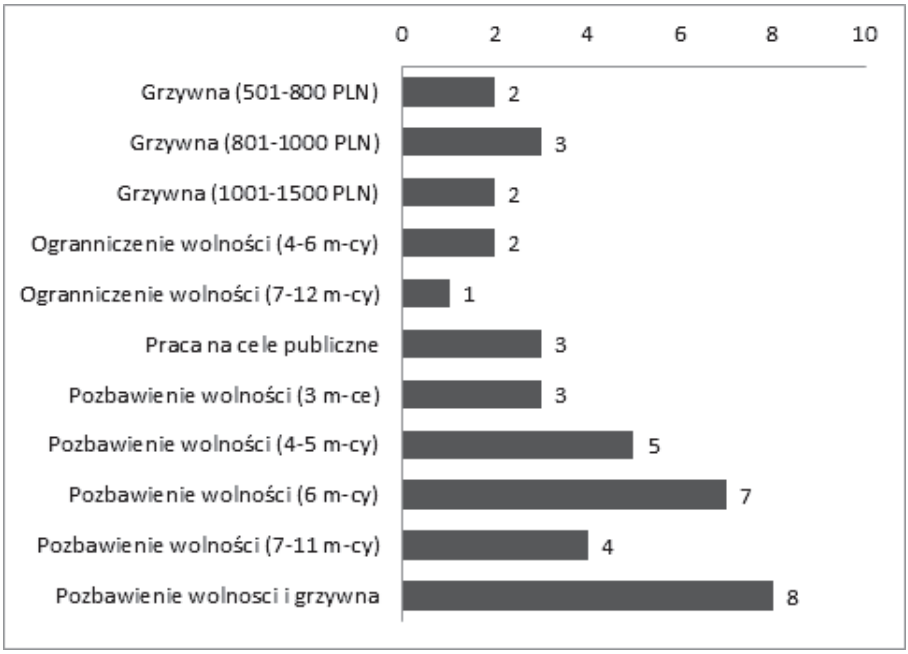
Rysunek 9. Liczba i odsetek osób skazanych za sabotaż komputerowy (art. 269a k.k.)



Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

W 2014 roku za naruszenie artykułów 268 k.k. i 268a k.k., orzeczono aż 19 kar pozbawienia wolności. Dodatkowo ośmiokrotnie orzekano o połączeniu kary pozbawienia wolności z karą grzywny. Samą karę grzywny sąd wymierzył 5 razy, a jej poziom kształtował się w przedziale 501–1500 złotych. Ograniczenie wolności orzeczono 3 razy. Sąd orzekł wobec sprawców prace na cele publiczne również 3 razy.

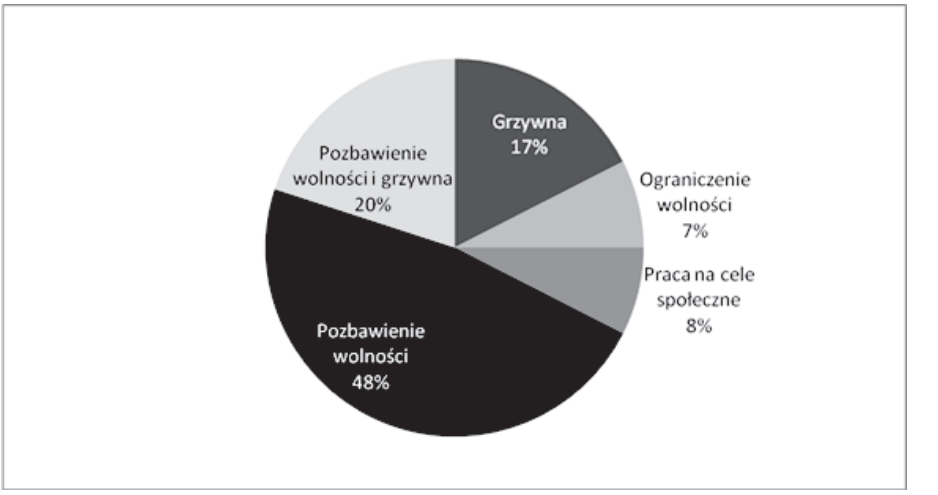
Rysunek 10. Wymiar kary w zakresie udaremniania i utrudniania korzystania z informacji z art. 268k.k. i 268a k.k. w roku 2014



Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

Dominowała zatem kara pozbawienia wolności, którą sądy orzekały za naruszenie artykułów 268 k.k. i 268a k.k. niemal w co drugim przypadku (zob. rys. 11). Dodatkowo karę pozbawienia wolności wraz z karą grzywny sądy orzekały w co piątym przypadku. Karę grzywny orzecznictwo w siedemnastu procentach, prace na cele społeczne w ośmiu procentach, a ograniczenie wolności w siedmiu procentach przypadków.

Rysunek 11. Odsetek kar i środków karnych orzekanych za przestępstwa popełnione z art. 268 k.k. i 268a k.k. w 2014 roku

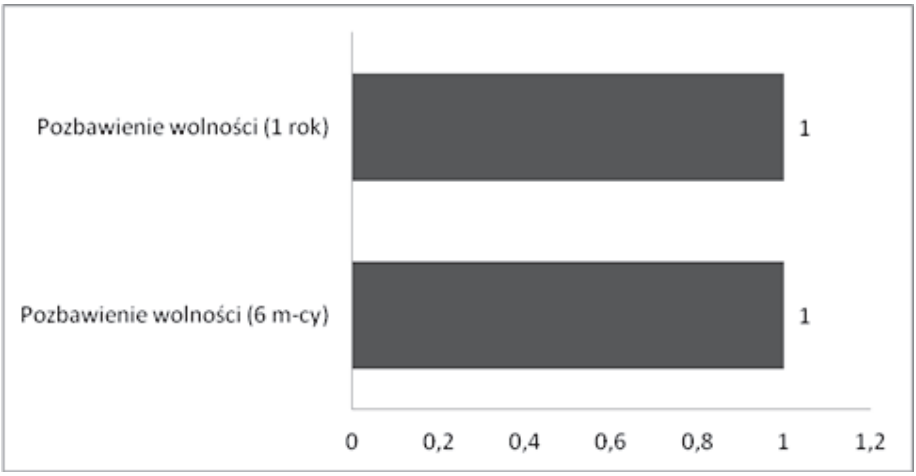


Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

W przypadku kar wymierzanych przez sądy za przestępstwa z art. 269a k.k. i 269b k.k., należy zauważyć, że w 2014 roku orzeczono tylko dwie takie kary (rys. 12). Były to: kara pozbawienia wolności na okres 1 roku i kara pozbawienia wolności na okres 6 miesięcy.

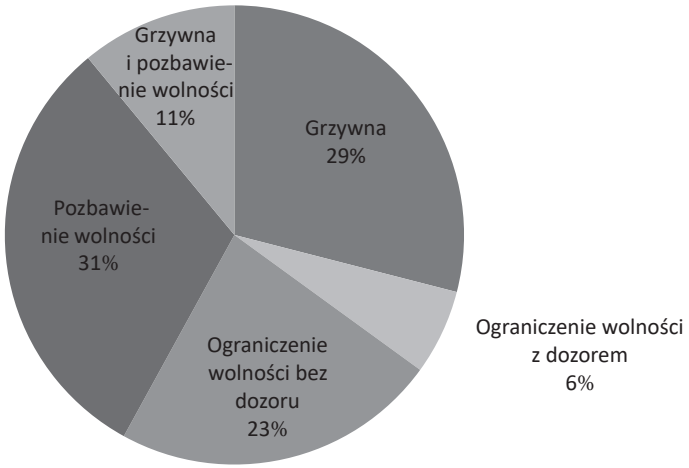
Podsumowując informacje odnoszące się do rodzaju wymierzonych kar w 2014 roku, będących następstwem popełnienia przestępstw przeciwko ochronie informacji, wskazuje się, że w 50 przypadkach orzeczono karę pozbawienia wolności, a w 23 karę pozbawienia wolności w połączeniu z karą grzywny. Karę grzywny orzeczono w 43 przypadkach. Ograniczenie wolności bez dozoru orzeczono w 37 przypadkach, a z dozorem w 9 przypadkach. Karą dominującą jest zatem pozbawienie wolności, którą orzeczono w prawie co trzecim przypadku (31%) – rys. 13. Dodatkowo często sądy decydowały się na orzekanie tej kary w połączeniu z grzywną (14%). Karę grzywny orzekano w co czwartym przypadku, podobnie jak ograniczenie wolności bez dozoru. Jednocześnie tylko co dwudziesty skazany w roku 2014 doświadczył ograniczenia wolności z dozorem.

Rysunek 12. Wymiary kar orzekanych przez sądy za sabotaż komputerowy i niszczenie danych informatycznych z art. 269a k.k. i 269b k.k. w roku 2014



Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

Rysunek 13. Wymiar kary zastosowany za przestępstwa przeciwko ochronie informacji w roku 2014



Źródło: *Opracowanie własne na podstawie: https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/ (dostęp: 18.05.2017)*

Należy podkreślić, iż w 2014 roku sądy za przestępstwa popełnione przeciwko ochronie informacji nie orzekały środków karnych w postaci zakazu zajmowania stanowisk czy zakazu wykonywania zawodu.

Wnioski de lege lata i de lege ferenda

Analizując zebrane dane statystyczne, należy stwierdzić, iż w przypadkach orzekania o przestępstwach przeciwko ochronie informacji w instytucjach publicznych w zakresie wydawanych orzeczeń o winie dominowały kary pozbawienia wolności i kary grzywny. Kara ograniczenia wolności z orzeczeniem dozoru orzekana była bardzo rzadko, tj. w co dwudziestym przypadku skazania. Jednocześnie sądy nie orzekały zakazu pełnienia funkcji publicznych czy zajmowania określonych stanowisk wobec osób, które dopuściły się tego rodzaju czynów, co powinno być naturalnym następstwem prawomocnego skazania.

Z przeprowadzonej analizy danych statystycznych udostępnionych przez Ministerstwo Sprawiedliwości i Policję można wnioskować, iż w sprawach o przestępstwa przeciwko ochronie informacji w instytucjach publicznych zapada niewielka liczba orzeczeń skazujących Nie należy jednak w sposób jednoznaczny upatrywać w tym aspekcie głównego powodu małej liczby wyroków skazujących w stosunku do liczby przestępstw zgłaszanych Policji. Nawet najlepiej sformułowane procedury dostępu do danych osobowych oraz zabezpieczenia ich przed nieuprawnionym ujawnieniem nie dają pełnej gwarancji przestrzegania prawa w tym zakresie. Od Policji, prokuratury i sądów zależy, czy zapisy zawarte w ustawach nie będą jedynie „martwymi normami prawa". Obok takich narzędzi jak przepisy prawa karnego, dodatkowo trzeba brać pod uwagę m.in. działania podejmowane przez organy ściągania. Należy także, w organizacjach publicznych, przestrzegać standardów dotyczących etyki zawodowej, działań organizacyjnych, w tym kontrolnych, monitoringu wewnętrznego i wysoce sprecyzowany na szczeblu kierownictwa zasad postępowania z danymi objętymi ochroną.

Literatura

1. Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, Strasburg 28 stycznia 1981, Dz.U. 2003 nr 3 poz. 25 z późn. zm.

2. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności Rzym, 4 listopada 1950, zmieniona Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993 nr 61 poz. 284 z późn. zm.
3. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych, Dz. Urz. WE L 281 z 21.11.1995, P. 0031.
4. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze komunikacji elektronicznej, Dz. Urz. L 201 z 31.07.2002, P. 0037–0047.
5. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997, Dz.U. 1997 nr 78 poz. 483 z późn. zm.
6. Ustawa z dnia 23 kwietnia 1964, Kodeks cywilny, Dz.U. 1964 nr 16, poz. 93 z późn. zm.
7. Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych, Dz.U. 1997 nr 133 poz. 883 z późn. zm.
8. Wyrok ETPCz z 16 lutego 2000 w sprawie Amann p. Szwajcarii Recueil des arrêts et décisions, 2000-II.
9. Wyrok ETPCz z 6 czerwca 2006 w sprawie Segerstedt-Wiberg and Others przeciwko Szwecji, Skarga nr 62332/00.
10. Wyrok ETPCz z 26 marca 1987 w sprawie Leander p. Szwecji, Skarga nr 9248/81.
11. Wyrok ETPCz w sprawie Segerstedt-Wiberg.
12. Wyrok ETPCz z 22 września 1993 w sprawie Klass, Sygn. 27/1992/372/446.
13. Wyrok ETPCz z 4 maja 2000 w sprawie Rotaru, Skarga nr 28341/95.
14. T.R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej*, Warszawa 2004.
15. Fischer B., *Administrator danych osobowych po przystąpieniu Polski do Unii Europejskiej. Uwagi de lege lata*, „Radca Prawny" 2005, nr 5.
16. A. Gliszczyńska-Grabias, K. Sękowska-Kozłowska, *Prawo do prywatności*, [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych*, Wieruszewski R. (red.), Warszawa 2011.
17. G. Szpor, *Publicznoprawna ochrona danych osobowych*, PUG 1999, nr 12.

PROTECTION OF PERSONAL DATA AND INFORMATION RIGHTS – CONSEQUENCES OF INFRINGEMENT OF PERSONAL DATA PROTECTION PROVISIONS

Summary: The article contains considerations concerning the protection of personal data included in the provisions of Polish law and international regulations. It raises the question of the right to collect information about citizens by public authorities. It contains interpretations of judgments of the European Court of Human Rights in Strasbourg and in particular the Act of 29 August 1997 on the protection of personal data. It also includes statistical data on initiated proceedings and offenses committed in relation to: hindering public authorities from accessing information, destroying data, computer sabotage, production of computer software destined for cybercrime. In the article the author also focuses on the analysis of the number of valid convictions adjudicated by the courts for such offenses and the types of penalties declared for committing them in the last twelve years.

Keywords: protection of personal data, right to information, crime against information protection, penalties for crime against information protection

Translated by Anna Słowik