O odpowiedzialności karnej administratorów bezpieczeństwa informacji

Karol Górski

Ultrasec

Wstęp

Wycieki danych osobowych są codziennością

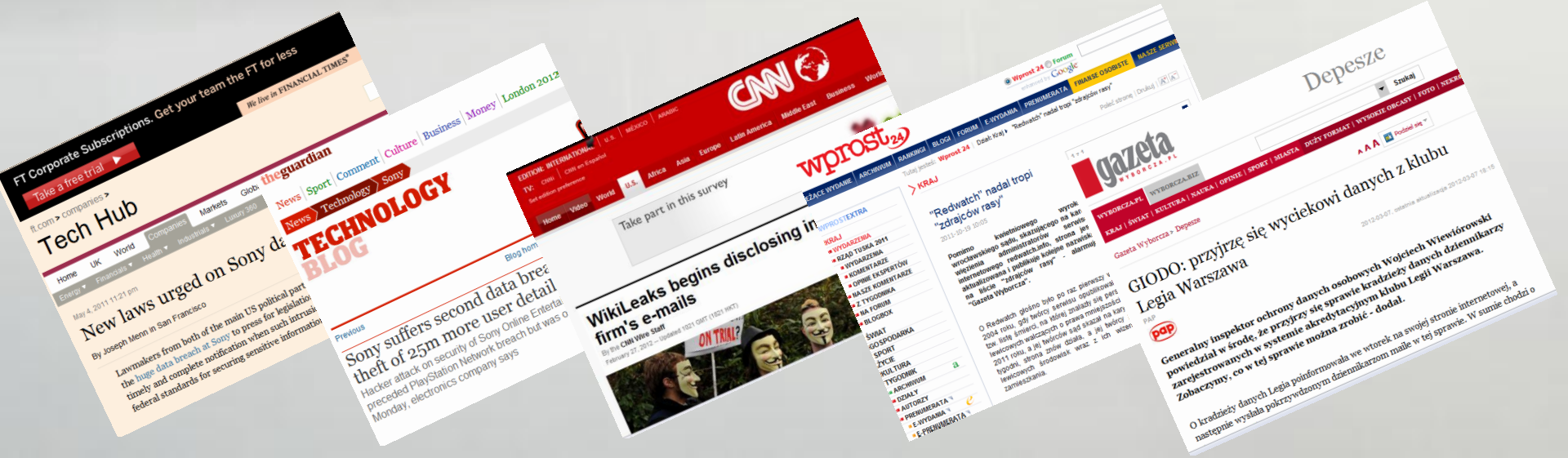
W USA wycieka ok. 300 mln. rekordów rocznie (dane sprzed kilku lat)

www.privacyrights.org/data-breach

przypadkowo spowodowane vs. celowe działania grup przestępczych

Niektóre powodują drobne uciążliwości (np. spam), niektóre wymierne szkody (kradzież tożsamości), niektóre mogą powodować tragedie

Po stronie podmiotów przetwarzających - koszty



Wstęp

Większość osób zgodzi się zapewne z postulatem karania bezpośrednich sprawców tych wycieków

A co z osobami, które przyczyniły się do niewystarczającego poziomu zabezpieczenia danych ?

W tym kontekście karanie za umyślne działania (sprawstwo i pomocnictwo, działania lub zaniechania) wydaje się oczywiste – trudniej natomiast określić zasady odpowiedzialności za czyny popełnione nieumyślnie

Wstęp

Czy należy karać za nieumyślne umożliwienie lub ułatwienie naruszenia bezpieczeństwa danych osobowych:

Administratorów systemów ?

Informatyków i programistów ?

Administratorów bezpieczeństwa ?

Użytkowników ?

Odpowiedzialność za nieumyślne działania/zaniechania pomaga określić wymagany poziom staranności tych osób

Wstęp

W pierwszym rzędzie warto się zastanowić nad odpowiedzialnością tych grup zawodowych, których podstawowa działalność wiąże się z bezpieczeństwem informacji

Karanie przedstawicieli tych grup zawodowych za nieumyślne działania lub zaniechania, skutkujące naruszeniem bezpieczeństwa danych, może być trudne przy wykorzystaniu obowiązujących norm prawa karnego

Jednak to nie oznacza, że inne osoby nie mogą ponieść odpowiedzialności za skutki tych działań lub zaniechań ani też, że osoby z tych grup zawodowych nie mogą ponieść odpowiedzialności innego rodzaju niż karna !

Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych

wykonanie dyrektywy UE 95/46

administracyjnoprawne uregulowanie przetwarzania danych osobowych

wyważenie interesów osób fizycznych i przedsiębiorców

określa

zasady dopuszczalnego przetwarzania danych osobowych
prawa osób których dane są przetwarzane
zasady nadzoru nad przetwarzaniem danych osobowych (GIODO)
kary za niezgodne z prawem przetwarzanie danych osobowych

3 rozporządzenia

1 istotne (zakres dokumentacji i podstawowe, wymagane zabezpieczenia)
2 mało istotne (wzór legitymacji i wzór wniosku o rejestrację)

Podstawowe pojęcia UODO

Dane osobowe

Dane „wrażliwe”

Przetwarzanie danych osobowych

Zbiór danych osobowych

Administrator danych osobowych
Administrujący danymi/zbiorem danych

Administrator bezpieczeństwa informacji

Kto może przetwarzać dane osobowe

Upoważnienie do przetwarzania danych osobowych

Wydane przez Administratora Danych

Tajemnica danych osobowych

Obejmuje dane osobowe i sposoby ich zabezpieczenia

Bezterminowa

Obowiązuje osoby upoważnione do przetwarzania d.o.

Możliwość powierzenia przetwarzania

AD jest wciąż odpowiedzialny za dane

Podmiot któremu powierzono przetwarzanie odpowiada za przetwarzanie niezgodnie z umową i za brak zabezpieczenia

Obowiązki administratora danych

Szczególna staranność AD !!!

Legalność, celowość, adekwatność i poprawność, ograniczenie czasowe

Zabezpieczenie danych

Obowiązek rejestracji zbioru danych

Ale szereg zwolnień – art. 43

Zwolnienie z obowiązku rejestracji nie zwalnia z pozostałych obowiązków w tym zabezpieczenia !!!

Obowiązek informacyjny

Niezależny od uzyskania zgody !!!

Obowiązki informacyjne, korekcyjne i zakazowe

Szczególna staranność

„W literaturze wyróżnia się jednak pięciostopniowy podział rodzajów staranności. Najniższym jej stopniem jest **minimalna** staranność (w granicach najniższego życiowego lub zawodowego doświadczenia), po której następuje: **niezbędna** (polegająca na wykonywaniu podstawowych czynności pracowniczych i zawodowych na podstawie wiedzy i umiejętności niezbędnych w konkretnym zawodzie), **należyta** (polegająca na dokonaniu wszystkich typowych czynności zgodnie z wyższymi umiejętnościami i kwalifikacjami), **szczególna** (mająca charakter kwalifikowany, zasadzająca się na dokonywaniu wszystkich możliwych czynności zgodnie z wysokimi kwalifikacjami) i **najwyższa** (możliwa do realizacji przy bardzo wysokich kwalifikacjach).”

„Wymóg ten zakłada każdorazową potrzebę konstruowania modelu działania o szczególnie surowych, wymagających kryteriach, stanowiących wzorzec, z którym porównywać należy kwestionowane zachowanie dziennikarza podczas wykorzystywania zebranych informacji. Wymóg szczególnej staranności to nakaz zachowania szczególnej, wyjątkowej ostrożności przy zbieraniu i wykorzystywaniu materiałów prasowych.”

(SN IV KKN 634/99)

Odpowiedzialność AD w związku z przetwarzaniem danych osobowych

Administracyjna

Decyzje (nakazy) GIODO po kontroli
Kontrole z urzędu lub na skutek skargi
Również za działania pracowników i podmiotów, którym powierzono przetwarzanie

Cywilna

Procesy o ochronę dóbr osobistych (AD, podmiot któremu powierzono przetwarzanie danych)

Odpowiedzialność osób fizycznych w związku z przetwarzaniem danych osobowych

Dyscyplinarna i porządkowa

Dotyczy pracowników
Porządkowa – wg przepisów KP
Dyscyplinarna – wg pragmatyk służbowych
Z inicjatywy pracodawcy lub na wniosek kontrolera

Urzędnicza

Dotyczy funkcjonariuszy publicznych
Za rażące naruszenie prawa
Charakter regresowy
Postępowanie wszczynane każdorazowo po wypłacie odszkodowania przez organ

Karna

Tylko osoby fizyczne, UODO nie jest wymienione w ustawie o odpowiedzialności podmiotów zbiorowych (dlaczego nie ?)
Z urzędu, na wniosek pokrzywdzonego lub GIODO lub innej osoby

Trochę statystyk dot. GIODO

	2007	2008	2009	2010	2011
Skargi	796	986	1049	1114	1272
Kontrole	167	201	220	196	199
Zawiadomienia o przestępstwie	18	31	27	18	9
Zbiory zgłoszone do rejestracji	4 850	5 776	7688	8260	15643
Zbiory zarejestrowane	2 598	3 760	6465	9921	11845

Obowiązek zabezpieczenia

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem

(art. 36 ust.1)

Administrator bezpieczeństwa informacji

Art.36 ust. 3

„Administrator danych wyznacza **administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1,** chyba że sam wykonuje te czynności”

Uważa się, że przypadek samodzielnego wykonywania zadań ABI przez AD dotyczy jednoosobowej działalności gospodarczej, w pozostałych przypadkach przyjmuje się że ABI powinien być osobą fizyczną zatrudnioną przez AD

W ustępie 1 nie ma mowy o „zasadach ochrony”

Ust. 1 „Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem”

Zakres obowiązków ABI

Co oznacza „nadzorowanie”

W prawie administracyjnym – kontrola + władcza ingerencja
Ale ABI występuje też w prywatnych podmiotach

Kwestia odpowiedzialności za zabezpieczenie danych osobowych

Czy można nadzorować swoją własną pracę ?
W większości miejsc nie jest to zadanie ABI ale czasami tak jest
Powoduje konflikt interesów

Jeśli zakres obowiązków jest szerszy niż w ustawie wtedy zakres odpowiedzialności może być inny !

Zakres faktycznie wykonywanych obowiązków vs. formalnie przypisany zakres obowiązków

Zakres odpowiedzialności karnej ABI

Interesują nas nieumyślne działania i zaniechania, które leżą w zakresie obowiązków ABI

Czy w grę wchodzi odpowiedzialność ABI z innych przepisów niż zawarte w UODO ?

Jaki jest zakres odpowiedzialności karnej ABI w porównaniu z osobami sprawującymi podobne funkcje w związku z innymi przepisami o ochronie informacji

Czyn umyślny i nieumyślny

1. *Czyn zabroniony popełniony jest umyślnie, jeżeli sprawca ma zamiar jego popełnienia, to jest chce go popełnić albo przewidując możliwość jego popełnienia, na to się godzi.*

2. *Czyn zabroniony popełniony jest nieumyślnie, jeżeli sprawca nie mając zamiaru jego popełnienia, popełnia go jednak na skutek niezachowania ostrożności wymaganej w danych okolicznościach, mimo że możliwość popełnienia tego czynu przewidywał albo mógł przewidzieć.*

(art. 9 KK)

Przestępstwo można popełnić nieumyślnie tylko wtedy, gdy ustawa tak stanowi

Warunki odpowiedzialności za czyny nieumyślne

Przy nieumyślności trzeba wykazać m.in. :

naruszenie reguł ostrożności

przewidywalność

związek przyczynowo-skutkowy (przy skutkowych)

Kto będzie ustalał jakie są reguły ostrożności wymagane w danych okolicznościach ?

dla ABI nie ma żadnych ogólnie przyjętych wymagań ani standardu postępowania

czy do reguł ostrożności należy przeprowadzanie testów penetracyjnych czy unikanie ich ?

czy kontrolę (audyt) należy prowadzić raz na tydzień czy raz do roku ?

czy w sytuacji gdy w oprogramowaniu zidentyfikowano lukę (podatność) ABI powinien spowodować wyłączenie systemu ? czy powinien śledzić informacje o podatnościach ?

Przewidywalność

„możliwość przypisania sprawcy skutków czynu obejmuje jedynie normalne, a niewykraczające poza możliwość przewidywania, następstwa jego zachowania” (SN IV KK 356/10)

Formy zjawiskowe przestępstwa

Sprawstwo indywidualne

Współsprawstwo

może być umyślne lub nieumyślne (wspólne naruszenie reguł ostrożności)

przy przestępstwie indywidualnym nie każdy współdziałający musi mieć wszystkie cechy indywidualizujące ale musi mieć wtedy świadomość, że inny współsprawca je posiada

Sprawstwo kierownicze i polecające

W literaturze dopuszcza się nieumyślną formę

Np. wydanie administratorowi systemu polecenia wyłączenia zabezpieczeń podczas prowadzonej przez ABI kontroli

Pomocnictwo (w tym przez zaniechanie) – tylko umyślnie

Podżeganie – tylko umyślnie

Sprawstwo przez zaniechanie

Przy przestępstwach skutkowych

Musi istnieć prawny, szczególny obowiązek zapobiegnięcia skutkowi (sprawca musi być „gwarantem” niedopuszczenia do skutku)

Obowiązek może wynikać z ustawy lub zobowiązania

Przy przestępstwach formalnych

Obowiązek działania wynika z ustawy

Czy „nadzorowanie przestrzegania zasad ochrony” jest prawnym, szczególnym obowiązkiem zapobiegnięcia np. udostępnieniu danych osobom nieupoważnionym ?

Odpowiedzialność karna ABI – wstępne podsumowanie

Rozważamy odpowiedzialność ABI za czyny nieumyślne popełnione w trakcie wykonywania ustawowo zakreślonych obowiązków (nadzorowanie przestrzegania przepisów)

Szukamy przepisów karnych wyraźnie stanowiących o odpowiedzialności z winy nieumyślnej

Wykluczamy pomocnictwo ze względu na wymóg umyślności

Mogą to być przestępstwa skutkowe lub formalne

Przy przestępstwach w formie zaniechań musi istnieć obowiązek nałożony na ABI odpowiadający takiemu zaniechaniu

przy skutkowych – obowiązek może wynikać z ustawy lub umowy (zobowiązania)

przy formalnych – obowiązek wynika z samego przepisu karnego

Przepisy karne UODO

Art.	Opis	Strona podmiotowa	Górny wymiar kary	Rodzaj
49	Nieuprawnione przetwarzanie	Umyślne	Do 3 lat	Formalne
51	Udostępnienie lub umożliwienie dostępu	Umyślne i nieumyślne	Do 2 lat	Formalne (?) i skutkowe
52	Naruszenie obowiązku zabezpieczenia	Umyślne i nieumyślne	Do 1 roku	Formalne
53	Niezgłoszenie zbioru do rejestracji	Umyślne	Do 1 roku	Formalne
54	Naruszenie obowiązku informacyjnego	Umyślne	Do 1 roku	Formalne
54a	Utrudnianie lub udaremnienie kontroli	Umyślne	Do 2 lat	Formalne i skutkowe

Udostępnienie osobom nieupoważnionym

Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

(Art. 51 ust. 1)

Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

(Art. 51 ust. 2)

Indywidualne/umyślne i nieumyślne/formalne (?) i skutkowe

Udostępnienie osobom nieupoważnionym

Wystarczy umożliwić dostęp – nie musi nastąpić

Udostępnienie można też traktować jako „uczynienie dostępnym”

Udostępnienie lub umożliwienie dostępu musi dotyczyć więcej niż jednej osoby

Choć są poglądy że tylko umożliwienie dotyczy wielu osób

Pojęcie „administrujący zbiorem/danymi”

Art. 51 dotyczy nie tylko zbioru danych

Upoważnienie do przetwarzania danych osobowych łączy się z obowiązkiem ich ochrony poprzez tajemnicę danych osobowych

Najczęściej zobowiązanie jest jawnie nakładane w drodze szkolenia, przepisów wewnętrznych itp.

Administrujący zbiorem / danymi

POSTANOWIENIE Z DNIA 11 GRUDNIA 2000 R.

II KKN 438/2000

[…]

2. Na gruncie ustawy o ochronie danych osobowych administratorem danych osobowych jest jedynie ten podmiot, który decyduje o celach i środkach przetwarzania tych danych (art. 7 pkt 4 ustawy), natomiast **administrującym - także taki podmiot, który zarządza, zawiaduje zbiorem danych (art. 50, 51, 54) lub danymi (art. 52) w procesie ich przetwarzania**, w tym i powierzonego mu w trybie wskazanym w art. 31 tej ustawy, przy czym odpowiedzialność karna administrującego nie będącego administratorem danych wchodzi w rachubę wówczas gdy jego zachowanie – uznane za karalne przez ustawę – wynika z powierzonych mu czynności przetwarzania danych.

Odpowiedzialność ABI z art. 51

Można przyjąć, że ABI jest osobą obowiązaną do ochrony danych (z samej nazwy i systematyki art. 36), nie jest jednak zazwyczaj administrującym zbiorem danych

Przykłady

Niedopilnowanie wdrożenia zabezpieczeń ?

Niesprawdzenie skuteczności zabezpieczeń ?

Niewstrzymanie przetwarzania po uzyskaniu informacji o luce bezpieczeństwa w oprogramowaniu systemu

Wyłączenie zabezpieczeń na czas kontroli

Odpowiedzialność ABI z art. 51 cd.

Trzeba udowodnić związek przyczynowo-skutkowy

Trzeba udowodnić, że ABI przewidywał lub mógł przewidywać, że jego działania lub zaniechania udostępnią lub umożliwią dostęp do danych

Przy zaniechaniach w przestępstwach skutkowych trzeba też udowodnić szczególny, prawny obowiązek zapobiegnięcia skutkowi

Istotne jest czy w obu odmianach (udostępnienia i umożliwienia) mamy do czynienia z przestępstwem skutkowym czy w drugiej odmianie (umożliwienie) jest to przestępstwo formalne

Niezabezpieczenie danych

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

(Art. 52)

Indywidualne/umyślne i nieumyślne/formalne

Niezabezpieczenie danych

Nie musi dojść do zabrania, uszkodzenia lub zniszczenia

Uszkodzenie, niszczenie lub kradzież danych (nośników) są objęte innymi przepisami KK

Sformułowanie sugeruje że chodzi o nośniki danych, które można zabrać, uszkodzić lub zniszczyć

Ale uszkodzenie lub zniszczenie danych może też nastąpić poprzez dostęp elektroniczny, bez skutku dla nośników

Dotyczy danych niezależnie od tego czy są w zbiorze czy nie

Dotyczy np. utraty pisma z danymi osobowymi

Odpowiedzialność ABI z art. 52

Czy o ABI można powiedzieć że administruje danymi ?

Raczej nie

Najczęściej ABI nie ma też obowiązku zabezpieczenia danych tylko nadzorowania czy dane są zabezpieczone

Inne źródła odpowiedzialności ABI

Funkcjonariusz publiczny, który, przekraczając swoje uprawnienia lub nie dopełniając obowiązków, działa na szkodę interesu publicznego lub prywatnego, podlega karze pozbawienia wolności do lat 3

(Art. 231 par.1 KK)

Jeżeli sprawca czynu określonego w par. 1 działa nieumyślnie i wyrządza istotną szkodę, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

(Art. 231 par. 3 KK)

Indywidualne/umyślne i nieumyślne/formalne i skutkowe

Czy ABI jest funkcjonariuszem publicznym ?

Funkcjonariusz publiczny (art. 115 KK) – m.in.:

[…]

osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych,

osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe,

osoba zajmująca kierownicze stanowisko w innej instytucji państwowej,

[…]

Czy ABI jest funkcjonariuszem publicznym ?

Sądy orzekały, że funkcjonariuszem publicznym jest m.in.

strażnik gminny (postanowienie SN z dnia 21 września 2005 r. sygn. I KZP 28/05)

asesor komorniczny – ale tylko gdy wykonuje określone czynności (uchwała SN z dnia 30 kwietnia 2003r., sygn. I KZP 12/03)

wójt gminy (jako pracownik samorządowy)

dyrektor przedsiębiorstwa państwowego (wyrok SN z dnia 13 marca 2007 r., sygn. WA 11/07)

zastępca dyrektora, główny specjalista, specjalista w Zarządzie Budynków Komunalnych (wyrok SN z 19 stycznia 2011 r., sygn. IV KK 356/10) (*)

Nie jest natomiast:

lekarz pogotowia ratunkowego (wyrok SN z dnia 27 listopada 2000 r. sygn. WKN 27/00)

leśniczy (postanowienie SN z dnia 8 grudnia 2004 r., sygn. IV KK126/04)

Funkcjonariusz publiczny wg ustawy o odpowiedzialności majątkowej funkcjonariuszy publicznych za rażące naruszenie prawa

Art. 2 ust. 1 pkt 1

Funkcjonariusz publiczny – osoba działająca w charakterze organu administracji publicznej lub z jego upoważnienia albo jako członek kolegialnego organu administracji publicznej lub osoba wykonująca w urzędzie administracji publicznej pracę w ramach stosunku pracy, stosunku służbowego lub umowy cywilnoprawnej, biorąca udział w prowadzeniu sprawy rozstrzyganej w drodze decyzji lub postanowienia przez taki organ

Odpowiedzialność ABI z art. 231 KK

ABI często nie są funkcjonariuszami publicznymi

Co to jest „istotna szkoda” ?

Art. 115 KK definiuje pojęcia „znacznej szkody” i „szkody w wielkich rozmiarach”

W przypadku pracowników instytucji państwowych i samorządowych można rozważyć zastosowanie art. 231 KK w związku z art. 304 par. 2 KPK (obowiązek zgłoszenia przestępstwa)

Czy zaniechanie zgłoszenia przez ABI przestępstwa to „istotna szkoda” ?

Art. 304. KPK

§ 1. Każdy dowiedziawszy się o popełnieniu przestępstwa ściganego z urzędu ma społeczny obowiązek zawiadomić o tym prokuratora lub Policję. Przepis art. 191 § 3 stosuje się odpowiednio.

§ 2. Instytucje państwowe i samorządowe, które w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten organ stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa.

Ustawa o ochronie informacji niejawnych

Ustawa z 5 sierpnia 2010 r.

Nie zawiera przepisów karnych

Szereg szczegółowych rozporządzeń

4 klasy informacji niejawnych

Informacje których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla interesów RP albo byłoby z punktu widzenia jej interesów niekorzystne

Zastrzeżone/poufne/tajne/ściśle tajne

Za ochronę IN odpowiada kierownik jednostki organizacyjnej

Tworzy wyspecjalizowaną komórkę – pion ochrony kierowany przez pełnomocnika ochrony

Dopuszczenie do IN – po uzyskaniu poświadczenia bezpieczeństwa osobowego w wyniku postępowania sprawdzającego i po przeszkoleniu

(w przypadku zastrzeżonych – zamiast poświadczenia wystarczy upoważnienie kierownika jednostki organizacyjnej)

Pełnomocnik ds. ochrony informacji niejawnych

Art. 14.

1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

2. Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego ***pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony", który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych****.*

Zadania POIN

Art. 15.

1. Do zadań pełnomocnika ochrony należy:

1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;

2) zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne;

3) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;

4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów;

5) opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;

Przepisy karne dot. informacji niejawnych

Art.	Opis	Strona podmiotowa	Górny wymiar kary	Rodzaj
265.1	Ujawnienie lub wykorzystanie informacji tajnych lub ściśle tajnych	Umyślne	Do 5 lat	Skutkowe
265.2	j.w. ale osobie działającej w imieniu lub na rzecz podmiotu zagranicznego	Umyślne	Do 8 lat	Skutkowe
265.3	Ujawnienie informacji tajnych lub ściśle tajnych	Nieumyślne	Do 1 roku	Skutkowe
266.1	Ujawnienie lub wykorzystanie informacji wbrew ustawie lub przyjętemu zobowiązaniu	Umyślne	Do 2 lat	Skutkowe
266.2	Ujawnienie informacji poufnych lub zastrzeżonych przez funkcjonariusza publicznego	Umyślne	Do 3 lat	Skutkowe
130.2	Udzielanie obcemu wywiadowi wiadomości, które mogą wyrządzić szkodę RP	Umyślne	Powyżej 3 lat	skutkowe
130.3	Gromadzenie lub przechowanie lub uzyskanie z systemu informatycznego wiadomości j.w. w celu udzielenia obcemu wywiadowi	Umyślne	Do 8 lat	Formalne (?) i skutkowe

Odpowiedzialność POIN

Art. 265 par. 3

Kto nieumyślnie ujawnia informację określoną w par. 1 [tj. informację niejawną o klauzuli „tajne” lub „ściśle tajne” – przyp. moje], z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

Sprawca musi zapoznać się z informacją, którą ujawnia !

O jakim upoważnieniu jest mowa w tym artykule ?

W UOIN upoważnienia występują w kontekście dopuszczenia do informacji zastrzeżonych oraz w kontekście kontroli prowadzonych przez funkcjonariuszy lub żołnierzy ABW/SKW

Odpowiedzialność POIN

Art. 231 par. 3

POIN stosunkowo częściej występują w instytucjach publicznych, ABI – częściej w firmach

POIN w firmie jest funkcjonariuszem publicznym tylko w zakresie postępowań sprawdzających (art. 115 par. 13) (dokładniej – wtedy gdy wydaje decyzje administracyjne)

Warunkiem jest wyrządzenie istotnej szkody

„ściśle tajne” – jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla RP

„tajne” – jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla RP

„poufne” – jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla RP

„zastrzeżone” – jeżeli ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań

Inspektor bezpieczeństwa teleinformatycznego

Art. 52 UOIN ust. 1 Kierownik jednostki organizacyjnej wyznacza:

1) pracownika lub pracowników pionu ochrony pełniących funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;

2) osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanych dalej „administratorem systemu”

Odpowiedzialność IBTI/AS

„Różnica obowiązków administratora systemu w stosunku do obowiązków inspektora bezpieczeństwa teleinformatycznego jest wyraźna i zasadnicza – ***administrator systemu odpowiada za każde uchybienie w funkcjonowaniu systemu lub niezgodność z zasadami i wymaganiami bezpieczeństwa****, a* ***inspektor bezpieczeństwa teleinformatycznego – co najwyżej za niewykonanie weryfikacji i kontroli****. Nie wymaga się nawet od niego, aby kontrola czy weryfikacja były skuteczne, tzn. aby odpowiadał za niewykryte w jej trakcie uchybienia”*

(S. Hoc: Ustawa o ochronie informacji niejawnych – komentarz, LexisNexis 2010, za T. Szewc: Ochrona informacji niejawnych. Komentarz, s. 260, 2007)

Czy dopuszczalna jest analogia z rolą ABI ?

Porównanie karalności z UODO i UOIN z winy nieumyślnej

	UODO	UOIN
Odpowiedzialność	UODO, KK	KK
Z winy nieumyślnej	51.2 UODO, 52 UODO, 231.3 KK	231.3 KK, 265.3 KK
Skrócony opis	51.2 – nieumyślne udostępnienie lub umożliwienie dostępu do danych osobowych 52 – nieumyślne naruszenie obowiązku zabezpieczenia danych osobowych przez zabraniem, uszkodzeniem lub zniszczeniem 231.3 – nieumyślne przekroczenie uprawnień lub niedopełnienie obowiązków i wyrządzenie istotnej szkody interesowi publicznemu lub prywatnemu (tylko funkcjonariusz publiczny)	231.3 – nieumyślne przekroczenie uprawnień lub niedopełnienie obowiązków i wyrządzenie istotnej szkody interesowi publicznemu lub prywatnemu (tylko funkcjonariusz publiczny) 265.3 – nieumyślne ujawnienie informacji tajnych lub ściśle tajnych (warunek zapoznania się z nimi)
Maks. kara	2 lata (51.2), 1 rok (52), 2 lata (231.3)	2 lata (231.3), 1 rok (265.3)
Przez nieumyślne zaniechanie	51.2, 52, 231.3	231.3, 265.3

Porównanie karalności ABI, POIN i IBTI z winy nieumyślnej

	ABI	POIN	IBTI
Zadania	Nadzorowanie przestrzegania zasad ochrony	Zapewnienie przestrzegania przepisów o ochronie informacji niejawnych; zapewnienie ochrony informacji niejawnych; zapewnienie ochrony systemów teleinformatycznych; kontrola OIN oraz przestrzegania przepisów	Weryfikacja i bieżąca kontrola zgodności funkcjonowania ST z SWB oraz przestrzegania PBE
Funkcjonariusz publiczny	Zależy od miejsca zatrudnienia	Zależy od miejsca zatrudnienia / tak - w zakresie postępowań sprawdzających	Zależy od miejsca zatrudnienia
Podstawa ukarania za nieumyślne przyczynienie się do zdarzenia	51.2 – tak ale trudne wykazanie statusu gwaranta, przewidywalności, związkuprzyczynowo-skutkowego 231.3 – trudne wykazanie związku przyczynowo-skutkowego i status gwaranta, do wykazania „wyrządzenie istotnej szkody”	231.3 – tak ale do wykazania „wyrządzenie istotnej szkody” 265.3 – raczej nie ze względu na wymóg zapoznania się z informacją	231.3 – trudne wykazanie związku przyczynowo-skutkowego i status gwaranta 265.3 – raczej nie ze względu na wymóg zapoznania się z informacją

Prawomocne skazania osób dorosłych w 2009 roku

Art.	Ogółem skazani	Grzywna	Ograniczenie wolności	Ograniczenie wolności z zawieszeniem	Pozbawienie wolności	Pozbawienie wolności z zawieszeniem
49/1	8	2	-	-	6	5
49/2	1	1	-	-	-	-
51	1	1	-	-	-	-
51/1	9	6	1	-	2	2
51/2	1	1	-	-	-	-
52	3	2	-	-	1	1
53	3	1	1	1	1	-
Łącznie	26	14	2	1	10	8

1*3 mies. bez zaw., 1*3 mies. w zaw., 5*4-5 mies. w zaw., 1*4-5 mies. bez zaw., 1*7-11 mies. w zaw., 1*1 rok w zaw.

* wszystkie artykuły z ustawy o ochronie danych osobowych

Prawomocne skazania osób dorosłych w 2010 roku

Art.	Ogółem skazani	Grzywna	Ograniczenie wolności	Ograniczenie wolności z zawieszeniem	Pozbawienie wolności	Pozbawienie wolności z zawieszeniem
49/1	8	3	-	-	5	5
49/2	1	-	-	-	1	1
51/1	9	8	-	-	1	1
51/2	2	2	-	-	-	-
52	1	1	-	-	-	-
53	4	4	-	-	-	-
54	1	1	-	-	-	-
Łącznie	26	19	-	-	7	7

1*3 mies. w zaw., 2*6 mies. w zaw., 1*7-11 mies. w zaw., 3*1 rok w zaw.

* wszystkie artykuły z ustawy o ochronie danych osobowych

Prawomocne skazania osób dorosłych w 2010 roku

	Skazani	Grzywna	Ogr. wolności	Ogr. zawiesz.	Pozb. wolności	Pozb. zawiesz.
265.1	4	-	-	-	4	4
266.1	43	14	7	1	22	21
266.2	4	-	-	-	4	4
267.1	52	35	5	1	12	12
267.3	11	9	-	-	2	2
267.3 w zw. z 1	2	1	-	-	1	-
267.3 w zw. z 1 małoletni	2	2	-	-	-	-
268.1	12	4	1	-	7	6
268.2	11	4	2	-	5	4
268.3	1	1	-	-	-	-

* wszystkie artykuły z kodeksu karnego

Prawomocne skazania osób dorosłych w 2010 roku

	Skazani	Grzywna	Ogr. wolności	Ogr. zawiesz.	Pozb. wolności	Pozb. zawiesz.
268a.1	33	11	8	3	14	14
268a.2	1	-	-	-	1	1
269.1	1	-	-	-	1	1
269.2	1	-	-	-	1	1
269a	3	1	-	-	2	2
269b.1	1	-	1	-	-	-
231.1	115	10	-	-	105	103
231.2	83	1	-	-	82	80
231.3	1	-	-	-	1	1
23.1	2	1	1	1	-	-
23.2	1	-	-	-	1	1

* art. 23 z ustawy o zwalczaniu nieuczciwej konkurencji, pozostałe z kodeksu karnego

Wnioski

Wbrew wyrażanym czasem opiniom podstawy odpowiedzialności karnej ABI/POIN/IBTI za czyny nieumyślne mogą być trudne do znalezienia

UODO wydaje się być bardziej represyjna niż UOIN w stosunku do osób popełniających nieumyślne przestępstwa

Zakres odpowiedzialności może zależeć od posiadania statusu funkcjonariusza publicznego