WPŁYW USTAWODAWSTWA AMERYKAŃSKIEGO NA ROZWÓJ RYNKU UBEZPIECZEŃ CYBERNETYCZNYCH W USA[1]

Wprowadzenie

Według raportu „*The Global Risks Report 2016*" przygotowanego dla Światowego Forum Ekonomicznego w Davos w styczniu 2016 r., cyberataki stanowią najpoważniejsze zagrożenie dla prowadzenia działalności gospodarczej w najbardziej rozwiniętych gospodarkach rynkowych, takich jak USA, Japonia, Niemcy, Szwajcaria, Holandia, Malezja [WEF 2016].

Tymczasem globalna skala przetwarzania elektronicznych danych osobowych stale rośnie, głównie w konsekwencji masowości urządzeń elektronicznych z dostępem do internetu, popularności portali społecznościowych, zakupów w sieci, bankowości elektronicznej, rozbudowanych transferów danych w sektorze przedsiębiorstw, a nade wszystko – zwiększania mocy obliczeniowej komputerów zdolnych do przetwarzania ogromnych zbiorów danych. Rozwój telefonii komórkowej oraz technologii GPS umożliwił poszerzenie katalogu danych osobowych nadających się do elektronicznego przetwarzania o informacje geolokalizacyjne czy szczegółowe profile konsumenckie. Jednocześnie metody gromadzenia danych osobowych stają się coraz bardziej wyrafinowane i trudniej wykrywalne [Komisja Europejska 2010].

Procesy te stwarzają zagrożenia, na które odpowiedzią jest tworzenie regulacji mających na celu zapewnienie odpowiedniego standardu ochrony prywatności, których konkretyzacją jest ochrona danych osobowych [Krzysztofek 2014]. Przepisy te nakładają na administratorów danych pewne obowiązki w zakresie zapewnienia bezpieczeństwa przechowywanych danych osobowych i odpowiedzialność za ich niespełnienie, a to z kolei w prosty sposób kieruje uwagę zainteresowanych w stronę rozwiązań ubezpieczeniowych, które gwarantują pokrycie strat wynikających z tego tytułu.

W literaturze wymienia się cztery przesłanki wprowadzania regulacji o obowiązku notyfikacji w razie naruszenia bezpieczeństwa danych osobowych[2] [Burdon *et al.* 2010; Smyth 2013]:

[1] Publikacja została sfinansowana ze środków przyznanych Wydziałowi Finansów i Prawa Uniwersytetu Ekonomicznego w Krakowie w ramach dotacji na utrzymanie potencjału badawczego.

[2] Naruszenie bezpieczeństwa danych osobowych określane jest w terminologii amerykańskiej jako „data breach". Wyrażenie to będzie wykorzystywane w niniejszej pracy.

- napiętnowanie dobrego imienia tych podmiotów, w których standardy zarządzania bezpieczeństwem informacji są na niewystarczającym poziomie oraz stworzenie impulsu stymulującego do podwyższania tych standardów,
- ochrona interesów konsumentów w obszarze bezpieczeństwa danych osobowych, prawa konsumentów do kontroli sposobu ich wykorzystania i przekazywania osobom trzecim,
- ograniczenie potencjalnych szkód wynikających z wycieku danych osobowych dzięki możliwie sprawnemu przeprowadzeniu operacji notyfikacji poszkodowanych (co pozwoli im na szybką reakcję np. zmiana haseł, zastrzeżenie kart kredytowych, monitorowanie przepływów finansowych na kontach bankowych),
- wzrost zaufania do instytucji zajmujących się gromadzeniem i przetwarzaniem danych.

Obowiązek notyfikacji, stanowiący fundament norm o ochronie danych osobowych, ma na celu wyraźne przypisanie odpowiedzialności za posiadane dane wszystkim tym podmiotom, które w ramach prowadzonej działalności administrują danymi osobowymi. To nie zawsze musi oznaczać penalizowanie przypadków wycieku danych, co ma powszechnie miejsce w USA. Nadmierne zagrożenie sankcjami mogłoby bowiem zniechęcić część podmiotów do wywiązywania się z obowiązku notyfikacji.

Poziom popytu na ubezpieczenia cybernetyczne w USA dalece odbiega *in plus* od innych krajów (przypis składki w Europie stanowi około 10% wartości składki pozyskanej z cyber ubezpieczeń w USA). Poszukując czynników determinujących tempo rozwoju rynku cyber ubezpieczeń można wskazać dwa najważniejsze: regulacje prawne dotyczące obowiązku notyfikacji w razie incydentu naruszenia bezpieczeństwa danych osobowych oraz publikacje w mediach informujące o dużych, a czasem spektakularnych przypadkach wycieku poufnych danych osobowych. Ten pierwszy czynnik ma jednak charakter fundamentalny, gdyż bez odpowiednich przepisów wymuszających ujawnianie *data breach* prawdopodobnie większość informacji o tego typu incydentach nie ujrzałaby światła dziennego ze względu na ogromne zagrożenie dla reputacji podmiotów doświadczających ataku hakerskiego. Można zatem podejrzewać, że implementacja przepisów o ochronie danych osobowych nakładających obowiązek notyfikacji w razie *data breach*, a także towarzyszące temu kary administracyjne, grzywny lub inne formy sankcji finansowych w razie niedopełnienia obowiązku notyfikacji są pierwotnym i wysoce relewantnym impulsem rozwoju rynku ubezpieczeń cyber na danym obszarze.

Wobec powyższych okoliczności sformułowano następujące pytanie badawcze: Czy regulacje prawne dotyczące *data breach* w USA są stymulantą rozwoju rynku ubezpieczeń cybernetycznych w USA?

Jego rozwiązanie stanie się możliwe dzięki zastosowaniu metod badawczych polegających na analizie prawodawstwa amerykańskiego (stanowego i federalnego) oraz na analizie rynku ubezpieczeń cybernetycznych w USA.

Celem pracy jest zatem analiza roli regulacji prawnych w stymulowaniu popytu na cyber ubezpieczenia na przykładzie doświadczeń USA.

Niniejszy artykuł wnosi do dotychczasowego dorobku nauki pogłębioną analizę komparatywną prawodawstwa amerykańskiego, w szczególności stanowego, w zakresie odpowiedzialności za naruszenie bezpieczeństwa danych osobowych (*data breach*). Dzięki temu możliwa stała się weryfikacja często powtarzanej tezy, że normy prawne w obszarze bezpieczeństwa danych osobowych i zasad elektronicznego ich przetwarzania mogą stymulować rozwój ubezpieczeń cybernetycznych, których jedną z funkcji jest ochrona podmiotu przetwarzającego dane osobowe przed finansowymi skutkami kar administracyjnych i roszczeń osób trzecich z tytułu naruszenia poufności tych danych.

1. Regulacje prawne dotyczące ochrony danych osobowych przetwarzanych elektronicznie w USA

Amerykańskie prawo dotyczące ochrony danych osobowych przetwarzanych elektronicznie, które wprowadza sankcje finansowe za naruszenie bezpieczeństwa tych danych, nie stanowi spójnego systemu norm. Mamy raczej do czynienia z rozproszonym zbiorem przepisów szczegółowych na poziomie federalnym oraz stanowym. Jak pisze Krzysztofek [2014], „Poddanie ochrony danych osobowych w konkretnej dziedzinie przepisom prawa USA następuje, gdy dziedzina ta zostanie uznana za społecznie istotną, a prawo do prywatności w jej zakresie – za wymagające szczegółowego określenia". Suwerenność systemów prawnych poszczególnych stanów i wynikające z tego zróżnicowanie zastosowanych rozwiązań legislacyjnych stanowi interesujący obszar badawczy, zwłaszcza w kontekście odpowiedzialności podmiotów przetwarzających dane osobowe za naruszenie poufności tych danych, co z kolei ma bezpośredni wpływ na sektor ubezpieczeń.

1.1.Przegląd najważniejszych norm prawa federalnego USA

Na poziomie prawa federalnego na szczególną uwagę w kontekście omawianej problematyki zasługują dwa akty prawne, które odnoszą się do instytucji finansowych (Ustawa Gramm-Leach-Bliley) oraz branży medycznej (Ustawa HIPAA).

W 1999 r. uchwalono **ustawę Gramm-Leach-Bliley'a (w skrócie GLBA)**, zwaną również ustawą modernizującą usługi finansowe (*The Financial Services Modernisation Act*). Poza wieloma istotnymi postanowieniami, wprowadziła ona szczególną kontrolę nad sposobem wykorzystania prywatnych danych osobowych przez instytucje finansowe. W myśl Sekcji 501 GLBA instytucja finansowa jest zobligowana:

- zapewnić bezpieczeństwo i poufność danych klientów,
- chronić przed możliwymi do przewidzenia zagrożeniami dla bezpieczeństwa i integralności tych danych,
- chronić dane przed nieuprawnionym dostępem lub wykorzystaniem, które mogłoby doprowadzić jakiegokolwiek klienta do poważnego uszczerbku lub niedogodności.

W zakresie pojęcia „instytucje finansowe" mieszczą się głównie banki, a ponadto inne instytucje znacząco zaangażowane w świadczenie usług finansowych[3].

Nad przestrzeganiem postanowień ustawy czuwa Federalna Komisja Handlu (*Federal Trade Commission*, FTC), która ma prawo nakładania kar. Przepisy ustawy odnoszą się do danych finansowych dotyczących konkretnych osób, które podawane są przez klientów instytucjom finansowym, powstają w rezultacie dokonywania operacji finansowych przez klienta instytucji finansowej lub zostały w jakikolwiek inny sposób pozyskane przez instytucję finansową (jedynym wyjątkiem są dane powszechnie dostępne w przestrzeni publicznej).

Instytucja finansowa nie może, ani bezpośrednio ani poprzez swoje placówki partnerskie, ujawniać nieupoważnionym podmiotom trzecim spersonalizowanych danych finansowych podlegających ochronie, chyba że instytucja finansowa powiadomi klienta o tym fakcie. Klient ma jednak prawo nie wyrażenia zgody na przekazanie jego danych finansowych do podmiotu trzeciego. Instytucje finansowe mają obowiązek podawania do wiadomości klientów gromadzonych przez nich informacji finansowych, związanych ze świadczonym usługami finansowymi lub oferowanymi produktami finansowymi. Dane te przekazuje instytucja finansowa w momencie nawiązania relacji z klientem, a później regularnie co rok przez cały okres trwania współpracy.

[3] Ustawa zalicza do instytucji finansowych: banki, towarzystwa ubezpieczeń, biura maklerskie, fundusze inwestycyjne, instytucje pożyczkowe, kasy oszczędnościowe, realizacja przekazów pieniężnych, doradztwo finansowe i podatkowe, pośrednictwo kredytowe, windykacja należności, zarządzanie nieruchomościami, doradztwo zawodowe dotyczące pracy w branży finansowej.

GLBA nie przewiduje indywidualnego dochodzenia roszczeń odszkodowawczych na drodze cywilnej przez osoby poszkodowane w wyniku naruszenia bezpieczeństwa danych. Za nieprzestrzeganie ustawy GLBA grożą kary administracyjne, których wysokość jest uzależniona od rodzaju instytucji finansowej. Instytucja finansowa może zostać ukarana grzywną w wysokości nieprzekraczającej 100.000 USD za każde naruszenie ochrony danych finansowych (należy pamiętać, że w praktyce jeden wyciek danych może skutkować serią wielu naruszeń prywatności). Kadra kierownicza instytucji finansowej ponosząca odpowiedzialność za naruszenie ustawy może zostać ukarana grzywną w wysokości nieprzekraczającej 10.000 USD za każde naruszenie. W stosunku do kadry zarządzającej instytucji finansowej mogą zostać zasądzone dodatkowe sankcje w postaci kary pozbawienia wolności do 5 lat. Jeżeli w ciągu 12 miesięcy dojdzie do ponownego naruszenia ochrony danych osobowych, wymiar wyżej wymienionych kar ulega podwojeniu [Ecora 2016][4].

Celem **Ustawy HIPAA (***Health Insurance Portability and Accountability Act***),** uchwalonej w 1996 r. i znowelizowanej Ustawą HITECH z 2009 r. (*Health Information Technology for Economic and Clinical Health Act*), jest ochrona poufności indywidualnych danych medycznych poprzez stosowanie polityki prywatności oraz różnego rodzaju rozwiązań służących do zabezpieczenia danych przed nieuprawnionym dostępem. Zadaniem dostawców usług medycznych oraz innych podmiotów podlegających ustawie jest zapewnienie poufności, integralności i dostępności informacji medycznych.

Przedmiotem regulacji są tzw. chronione dane medyczne (*Protected Health Information*, PHI), definiowane jako spersonalizowane informacje o stanie zdrowia, podlegające przechowywaniu lub transmisji z wykorzystaniem mediów elektronicznych (z wyjątkiem danych wykorzystywanych w celach edukacyjnych oraz danych o pracownikach przechowywanych przez pracodawcę).

Zakres podmiotowy ustawy obejmuje szereg organizacji związanych bezpośrednio z ochroną zdrowia, jak również pośrednio – ich partnerów biznesowych (podwykonawców, kooperantów), w szczególności: lekarzy, domy opieki, apteki, towarzystwa ubezpieczeń zdrowotnych, instytucje ochrony zdrowia (HMO, *Health Maintanance Organisations*), firmy zewnętrzne dostarczające usługi dla służby zdrowia – o ile dochodzi do elektronicznej transmisji danych o stanie zdrowia (§160.103 HIPAA). Podmioty te są zobowiązane, w razie

[4] Zagrożenie sankcjami wobec banków jest jednak znacznie wyższe. Oprócz kar finansowych na poziomie 1 mln USD lub 1% aktywów, przewidziano także możliwość odwołania zarządu banku oraz pozbawienie winnych osób prawa do zasiadania w organach zarządzających jakiejkolwiek instytucji finansowej.

wypadku naruszenia bezpieczeństwa prywatnych danych o stanie zdrowia, powiadomić wszystkie osoby, których dane dotyczą, najpóźniej w ciągu 60 dni od dowiedzenia się o incydencie[5]. Obowiązki informacyjne są zróżnicowane w zależności od skali i zakresu naruszenia. Istnieje możliwość zwolnienia z procedury notyfikacji, jeśli po przeprowadzeniu analizy ryzyka wykaże się niewielkie prawdopodobieństwo tego, że doszło do ujawnienia PHI. Kolejną przesłanką wyłączającą obowiązek notyfikacji jest wykazanie, że dane medyczne, które zostały bezprawnie ujawnione, znajdują się w stanie uniemożliwiającym ich wykorzystanie, odczytanie lub zrozumienie (jest to tzw. zasada *safe harbor*, czyli zasada „bezpiecznej przystani"). Zgodnie z przepisami HIPAA warunek ten jest spełniony wyłącznie w dwóch przypadkach: jeśli dane były w odpowiedni sposób zaszyfrowane lub jeśli nośnik, na którym przechowywano przedmiotowe dane PHI, został zniszczony.

W przypadku, gdy liczba poszkodowanych przekroczy 500, należy dodatkowo zawiadomić najważniejsze media oraz Sekretarza Stanu ds. Zdrowia i Pomocy Społecznej (*Secretary of Health and Human Services*) [Smyth 2013].

Podmiot, który dopuścił się naruszenia bezpieczeństwa danych medycznych zagrożony jest grzywną nakładaną przez Sekretarza Stanu ds. Zdrowia i Opieki Społecznej. Wysokość grzywny uzależniona jest od liczby poszkodowanych oraz okoliczności wypadku. Jeśli do naruszenia doszło w wyniku nieświadomości popełniania czynu niedozwolonego, grzywna wynosi przynajmniej 100 USD za naruszenie, lecz łącznie nie więcej niż 1,5 miliona USD. W przypadku działania świadomego, grzywna wzrasta do minimum 1.000 USD za naruszenie, lecz łączna jej kwota nie może przekroczyć 1,5 miliona USD. Osobom poszkodowanym nie przyznano prawa do indywidualnego dochodzenia roszczeń odszkodowawczych na drodze cywilnej.

1.2. Analiza komparatywna prawa stanowego w USA

W odpowiedzi na rosnącą falę nadużyć w obszarze bezpieczeństwa przechowywanych przez różne organizacje danych osobowych niektóre stany USA rozpoczęły prace nad zbiorem przepisów wprowadzających odpowiednie zasady postępowania oraz sankcje karne za nieprzestrzeganie ustalonych norm. Pierwsze regulacje dotyczące *data breach* uchwaliła Kalifornia w 2002 r. (weszły w życie 1 lipca 2003). Tym tropem podążyły pozostałe stany, z

[5] Publikacja zawiadomienia o naruszeniu bezpieczeństwa danych medycznych może zostać czasowo wstrzymana, jeśli mogłoby to niekorzystnie wpłynąć na toczące się postępowanie sądowe.

wyjątkiem trzech (Nowy Meksyk, Dakota Południowa, Alabama). Ostatecznie do 2015 r. 48 stanów amerykańskich wprowadziło już takie regulacje.

Zasadnicze normy zawarte w prawodawstwie poszczególnych stanów są ze sobą zbieżne i z reguły wzorowane na pionierskich rozwiązaniach wprowadzonych w Kalifornii. Pewne różnice pojawiają się w przepisach szczegółowych i będą one przedmiotem rozważań w dalszej części opracowania.

Przepisy o obowiązku notyfikacji w razie naruszenia bezpieczeństwa danych dotyczą z reguły osób fizycznych lub osoby prawne, które prowadzą działalność gospodarczą na terenie danego stanu, a także instytucji publicznych, w których posiadaniu znajdują się przetwarzane komputerowo dane osobowe. Przez dane osobowe podlegające ochronie rozumie się zwykle imię lub inicjał imienia wraz z nazwiskiem, w połączeniu z takimi danymi jak:

a) numer ubezpieczenia społecznego,
b) numer prawa jazdy lub numer stanowego dowodu tożsamości (*state identification card*),
c) numer konta bankowego, karty kredytowej lub debetowej w połączeniu z wymaganymi hasłami dostępu, pin'ami i innymi formami autoryzacji dostępu,
d) informacje medyczne o stanie zdrowia lub przebiegu leczenia,
e) dane ubezpieczenia zdrowotnego.

Podmioty, które gromadzą, administrują lub przetwarzają dane osobowe (w powyższym rozumieniu) są zobowiązane zapewnić ich poufność i niemożność dostępu przez niepowołane osoby trzecie. Jednak w razie naruszenia bezpieczeństwa danych osobowych, rozumianego jako nieautoryzowane przejęcie danych elektronicznych, które narusza bezpieczeństwo, poufność lub integralność posiadanych przez ten podmiot danych osobowych, przedsiębiorca ma obowiązek niezwłocznie powiadomić o tym fakcie wszystkie osoby, które mogły lub mogą doznać uszczerbku w dobrach osobistych lub majątkowych. Warto dodać, że wymóg notyfikacji rozciąga się tylko na osoby poszkodowane zamieszkujące dany stan (rezydentów). Zawiadomienie powinno zostać wydane niezwłocznie po uzyskaniu wiadomości o wystąpieniu naruszenia, zaś preferowaną formą kontaktu jest forma pisemna. Powiadomienie poszkodowanych może zostać czasowo wstrzymane, jeśli jego publikacja mogłaby wpłynąć negatywnie na prowadzone postępowanie karne.

Wymóg powiadomienia w przypadku wycieku danych osobowych nie występuje, jeśli informacje te wyciekły w postaci zaszyfrowanej i nie doszło do ujawnienia metody szyfrowania (tzw. zasada *Encryption Safe Harbor*).

Najważniejsze różnice w ustawodawstwie poszczególnych stanów dotyczą takich kwestii, jak:

a) czas na powiadomienie o naruszeniu bezpieczeństwa danych osobowych,
b) uzależnienie obowiązku notyfikacji od wyników analizy stopnia zagrożenia stratami materialnymi (tzw. *harm threshold*),
c) podmioty instytucjonalne, których powiadomienie o naruszeniu jest obligatoryjne,
d) umiejscowienie prawa do nakładania lub dochodzenia sankcji cywilnych lub karnych za niedopełnienie obowiązku notyfikacji,
e) czy osoby prywatne, poszkodowane w wyniku *data breach*, mają prawo samodzielnego dochodzenia odszkodowania na drodze cywilnej,
f) rodzaje i tytuły nakładanych grzywien administracyjnych oraz ewentualne limity kwotowe.

W wielu przypadkach różnice te sprawiają, że podmiot zagrożony odpowiedzialnością za naruszenie bezpieczeństwa danych zostanie postawiony w zupełnie innej sytuacji prawno-finansowej, dlatego zdaniem autora uzasadnione jest dokładne zbadanie stopnia zróżnicowania przepisów stanowych.

W większości stanów (39) administrator danych zobowiązany jest do niezwłocznego powiadomienia wszystkich osób, których utracone dane osobowe dotyczyły, biorąc jednak pod uwagę czas potrzebny na ustalenie skali naruszenia i przywrócenie integralności systemu IT. Przepisy nie określają żadnego terminu granicznego, w którym procedura notyfikacji powinna zostać zakończona. Tylko nieliczne stany zdecydowały się na bardziej precyzyjne ujęcie okresu przewidzianego na publikację zawiadomienia. W regulacjach stanu Floryda wymienia się termin 30-dniowy od dowiedzenia się o incydencie, w Connecticut przewidziano termin 90-dniowy, zaś w sześciu innych stanach – okres 45-dniowy (OH, RI, TN, VT, WA, WI)[6].

Regulacje stanowe mogą przewidywać przeprowadzenie analizy prawdopodobieństwa wystąpienia strat materialnych w wyniku naruszenia bezpieczeństwa danych (tzw. *harm threshold*), dzięki której staje się możliwe odstąpienie od obowiązku powiadamiania poszkodowanych. Powiadomienie każdego poszkodowanego o naruszeniu danych osobowych nie jest wymagane, jeśli po zawiadomieniu stanowego prokuratora generalnego przeprowadzono analizę potencjalnych skutków wycieku danych i na jej podstawie stwierdzono, iż jest mało prawdopodobne lub wręcz niemożliwe, by osoby których dane dotyczą doznały w wyniku naruszenia poufności tych danych jakiegokolwiek uszczerbku. Jest to zatem ogromna szansa dla podmiotów, które doświadczyły wycieku poufnych danych osobowych, by uniknąć kosztownej procedury notyfikacji wszystkich dotkniętych skutkami

[6] Autor posługuje się standardowymi oznaczeniami literowymi stanów, których objaśnienia można znaleźć m.in. na stronie: www.zipcodecountry.com.

tego incydentu. Regulacje przewidujące dopuszczalność analizy „*harm threshold*" występują obecnie w 37 stanach. Tam, gdzie ustawodawca stanowy nie zdecydował się na to rozwiązanie, obowiązek notyfikacji powstaje w każdym przypadku, niezależnie od przewidywanych skutków negatywnych (są to stany: CA, DC, GA, IL, MN, NE, NV, NY, ND, TN, TX).

Skala ekspozycji na ryzyko osób poszkodowanych w wyniku nieautoryzowanego ujawnienia ich danych osobowych, a także zagrożenie nałożeniem na administratora danych odpowiedzialnego za ten incydent sankcji karnych i cywilnych powoduje, że o konkretnych przypadkach naruszeń obligatoryjnie zawiadamia się także wskazane w normach prawnych instytucje i organy stanowe.

Stanowy prokurator generalny zostaje notyfikowany o naruszeniu w następujących sytuacjach:

- w każdym przypadku naruszenia bezpieczeństwa danych osobowych (AK[7], CT, IN, LA, ME, MD, MA, MT, NE, NH, NY, NC, VA, VT),
- gdy liczba osób dotkniętych wyciekiem danych przekracza 250 (ND, OR),
- gdy liczba osób dotkniętych wyciekiem danych przekracza 500 (CA, IA, RI, WA),
- gdy liczba osób dotkniętych wyciekiem danych przekracza 1.000 (MO).

W 27 stanach nie wprowadzono obowiązku powiadamiania prokuratora generalnego.

Wystąpienie *data breach* z liczbą poszkodowanych przekraczającą określony pułap skutkuje w wielu stanach koniecznością niezwłocznego zawiadomienia największych, krajowych organizacji ochrony praw konsumentów. Powinność ta powstaje:

- w każdym przypadku naruszenia bezpieczeństwa danych osobowych (MA, MT),
- gdy liczba osób dotkniętych wyciekiem danych przekracza 500 (MN, RI),
- gdy liczba osób dotkniętych wyciekiem danych przekracza 1.000 (AK, CO, DC, FL, HI, IN, KS, KY, ME, MD, MI, MO, NV, NH, NJ, NC, OH, OR, PA, SC, TN, VA, VT, WI, WV),
- gdy liczba osób dotkniętych wyciekiem danych przekracza 5.000 (NY),
- gdy liczba osób dotkniętych wyciekiem danych przekracza 10.000 (GA, TX).

W 16 stanach nie przewidziano obligatoryjnego powiadamiania organizacji konsumenckich.

Wśród innych organów lub instytucji, które wymagają powiadomienia w określonych sytuacjach należy wymienić:

- stosowny organ nadzorujący branżę, w której prowadzi działalność podmiot, gdzie doszło do incydentu *data breach* (ME, NH, OK, VT),

[7] Powiadomienie prokuratora generalnego jest wymagane tylko wtedy, gdy osoby poszkodowane nie zostają notyfikowane z powodu zastosowania mechanizmu „*harm threshold*".

- Komisarz ds. Papierów Wartościowych (AR) – gdy naruszenie obejmuje dane finansowe lub numery ubezpieczenia społecznego kredytobiorców,
- Departament Prawny w administracji stanowej (FL, NY),
- stanowe Biuro Ochrony Konsumentów (HI, MA, MT, NC, SC),
- Departament Policji Stanowej (NJ, NY).

W przypadku dopuszczenia do naruszenia bezpieczeństwa danych osobowych administratorowi tych danych grożą różnego rodzaju sankcje karne o charakterze administracyjnym oraz odpowiedzialność odszkodowawcza wobec poszkodowanych osób, których dane dotyczą. Jedynie w pięciu stanach nie występują szczególne przepisy, które regulowałyby powyższe kwestie (GA, KY, MT, TN, WI). W pozostałych przypadkach przepisy stanowią, iż naruszenie ochrony danych osobowych traktowane jest zwykle jako niedozwolone praktyki rynkowe, zaś nakładanie kar administracyjnych albo wszczynanie postępowań karnych lub cywilnych w imieniu poszkodowanych leży w gestii stanowego prokuratora generalnego. Inicjatywa prawna w tym zakresie w sporadycznych przypadkach może należeć do prokuratora okręgowego (OK, VT) lub dyrektora departamentu zajmującego się sprawami konsumenckimi (OR, SC).

Jednym z fundamentalnych pytań w kwestii odpowiedzialności za naruszenie ochrony danych osobowych, zarówno dla podmiotów narażonych na sankcje, jak i dla towarzystw ubezpieczeń szacujących ryzyko związane z ubezpieczeniami cyber, jest wysokość potencjalnych kar i roszczeń odszkodowawczych. Analiza regulacji stanowych prowadzi do wniosku, że mamy do czynienia ze znacznym zróżnicowaniem dolegliwości sankcji finansowych w przypadku *data breach*. W 20 stanach nie sprecyzowano kwotowych limitów ograniczających nakładane sankcje finansowe, pozostawiając to uznaniu sądu[8]. Natomiast w 22 stanach regulacje określają górne kwoty kar administracyjnych w ujęciu łącznym, bądź w przeliczeniu na jednego poszkodowanego (tabela 1).

Tabela 1. Zestawienie kar administracyjnych za naruszenie bezpieczeństwa danych osobowych w USA (stan na 1 lipca 2016 r.)

Nazwa stanu USA	Maksymalna kara administracyjna (w USD)	
	Za 1 poszkodowanego	Łącznie
Alaska	500	50.000
Arizona	---	10.000
Dystrykt Kolumbii	100	---
Floryda	---	500.000
Hawaje	2.500	---
Idaho	---	25.000
Illinois	---	50.000

[8] AR, CA, CO, CT, DE, KS, MD, MA, MS, NE, NV, NH, NJ, NC, OH, OK, PA, VT, WA, WY.

Indiana	---	150.000
Iowa	---	40.000
Maine	500	2.500[1]
Michigan	250	750.000
Minnesota	---	25.000
Missouri	---	150.000
Nowy Jork	---	150.000[2]
Dakota Północna	5.000	---
Oregon	1.000	---
Rhode Island	100	25.000
Karolina Południowa	1.000	---
Teksas	50.000[3]	---
Utah	2.500	100.000
Wirginia	---	150.000
Wirginia Zachodnia	---	150.000[4]

Legenda:
1 – plus „stosowna rekompensata"
2 – tylko gdy wina umyślna lub rażące niedbalstwo
3 – plus kara administracyjna za opóźnienie notyfikacji
4 – tylko gdy wina umyślna

Źródło: opracowanie własne.

Z zestawienia zaprezentowanego w tabeli 1 wynika, że poziom kar administracyjnych jest niezwykle zróżnicowany. W przypadku dziewięciu stanów łączne sankcje nie przekroczą poziomu 100 tys. USD, zaś w kolejnych pięciu maksymalny ich pułap ustalono na 150 tys. USD, choć w Nowym Jorku i Wirginii Zachodniej nałożenie tych kar uzależnione jest od udowodnienia sprawcy winy umyślnej. Największe zagrożenie z punktu widzenia winnego naruszenia ochrony danych osobowych zlokalizowane jest w jurysdykcji Florydy i Michigan. Nie można również pominąć Teksasu, w którym tak wysoki poziom sankcji na jednego poszkodowanego wynika z faktu pozbawienia osób indywidualnych prawa do samodzielnego dochodzenia roszczeń odszkodowawczych na drodze cywilnoprawnej. Przypadki stanów, w których określono jedynie limity kar administracyjnych przypadających na każdego poszkodowanego, przy braku górnego ograniczenia łącznej wartości kary, stanowią poważne wyzwanie dla tych przedsiębiorstw, które przetwarzają znaczne zbiory danych osobowych – liczące setki tysięcy lub miliony rekordów.

Ostatnią, choć nie mniej ważną, kwestią znajdującą skrajne rozwiązania w poszczególnych stanach jest odpowiedź na pytanie, czy osoby prywatne, poszkodowane w wyniku *data breach,* mają prawo samodzielnego dochodzenia odszkodowania na drodze cywilnej. W większości stanów[9] (33 stany) takiej ścieżki odszkodowawczej nie przewidziano, a za dochodzenie roszczeń na rzecz poszkodowanych najczęściej odpowiada stanowy prokurator generalny.

[9] Stany: AZ, AR, CO, CT, DE, FL, GA, ID, IN, IA, KS, KY, ME, MA, MI, MS, MO, MT, NE, NV, NJ, NY, ND, OH, OK, PA, RI, TX, UT, VT, WV, WI, WY.

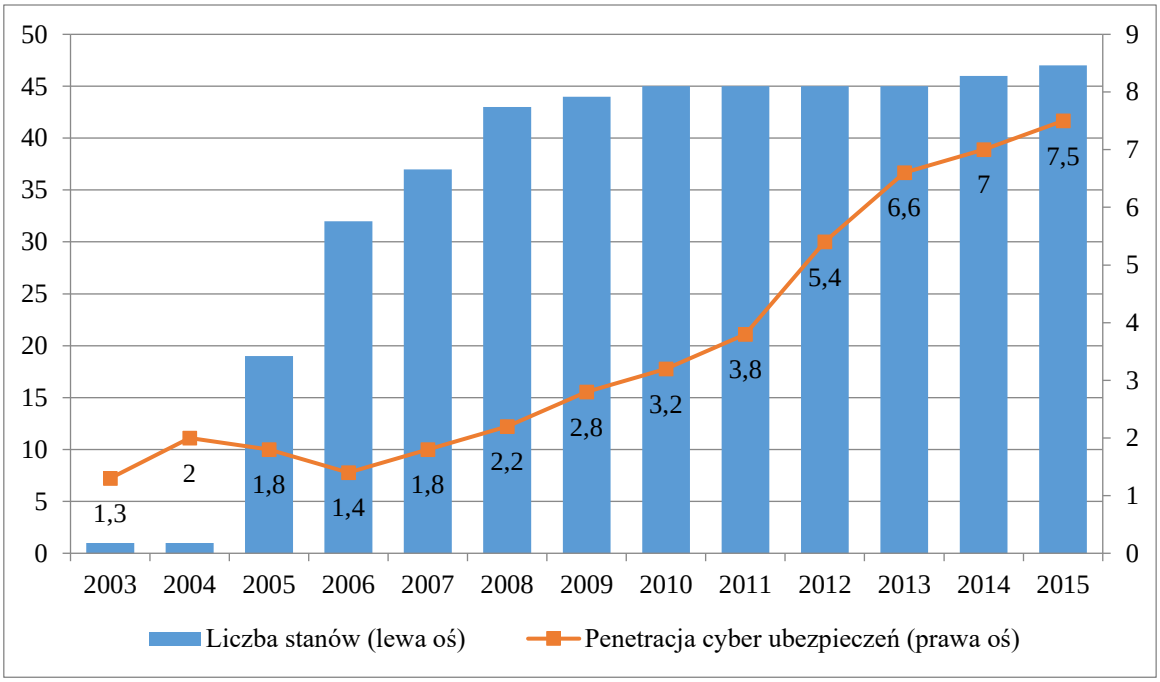
Przepisy w 10 stanach[10] dopuszczają indywidualne dochodzenie roszczeń za faktycznie poniesione straty wynikające z *data breach*, zaś rezydenci Dystryktu Kolumbii, Hawajów, Minnesoty i Karoliny Południowej poza roszczeniem typowo odszkodowawczym mogą ubiegać się dodatkowo o zwrot kosztów postępowania sądowego i kosztów ochrony prawnej. Warto odnotować, iż w przypadku indywidualnego dochodzenia odszkodowań na drodze cywilnoprawnej nie jest praktykowane ustawowe limitowanie pułapu odszkodowań. Tylko w jednym stanie, na Alasce, normy prawne określają górny limit roszczeń odszkodowawczych – 500 USD na osobę.

2. Wpływ regulacji na wielkość i strukturę rynku ubezpieczeń cybernetycznych w USA

Poważne zagrożenie sankcjami karnymi wobec przedsiębiorstw i innych instytucji postępujących niezgodnie z zasadami ochrony danych osobowych przewidzianymi w prawie federalnym i stanowym USA skutkują wykorzystaniem zróżnicowanych technik zarządzania ryzykiem, przede wszystkim technicznych i organizacyjnych narzędzi kontroli ryzyka IT. Zgodnie z raportem Instytutu SANS [2016], głównymi motywami alokacji funduszy badanych podmiotów w bezpieczeństwo IT były: ochrona danych wrażliwych (63% respondentów), zgodność z obowiązującymi przepisami (56%) oraz przeciwdziałanie incydentom naruszenia ochrony danych osobowych (31%). Natomiast łączne nakłady na cyber bezpieczeństwo stanowiły od 3% do 6% budżetu przedsiębiorstwa, z wyjątkiem sektora instytucji finansowych, gdzie poziom nakładów osiągał poziom 10-12%.

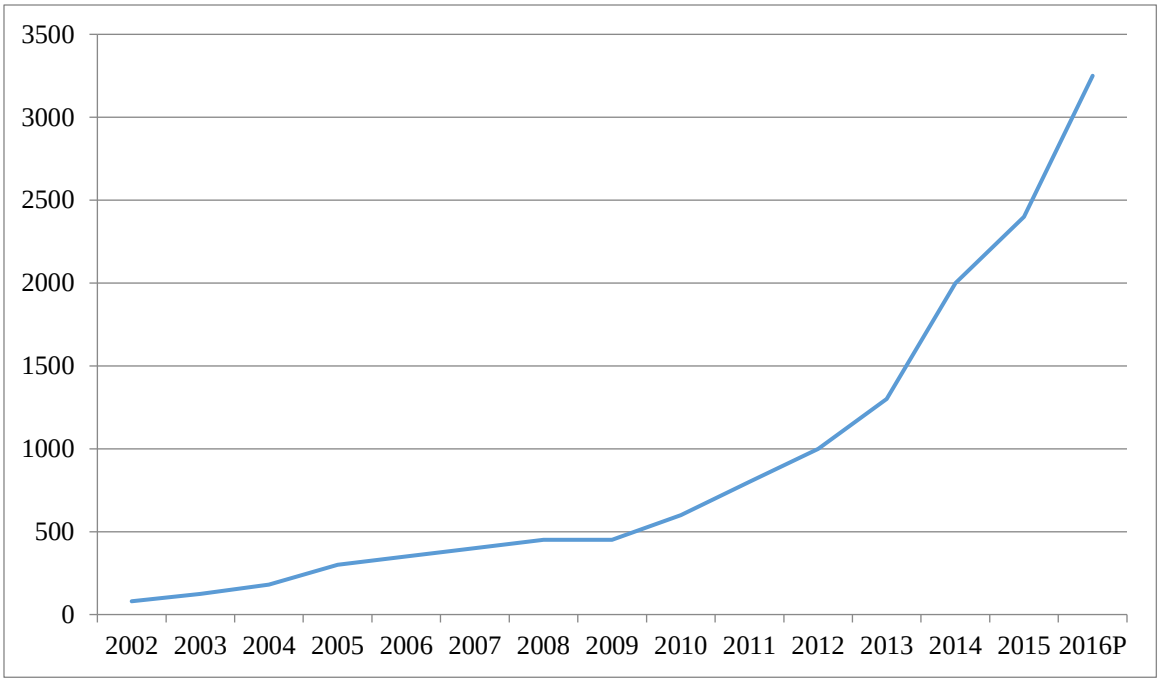
Wysokie zaangażowanie organizacji w ograniczaniu zagrożeń mających swe źródło w cyber przestrzeni, stymulowane w widoczny sposób przez regulacje prawne, przekłada się na stopniowy wzrost popytu na ubezpieczenia cybernetyczne. Prawdziwość tej hipotezy potwierdzają dane przedstawione na rysunku 1. W miarę uchwalania przez poszczególne stany USA przepisów o prawnej ochronie danych osobowych odnoszących się do obowiązku notyfikacji w razie *data breach*, wskaźnik penetracji cyber ubezpieczeń wzrastał z 1,3% w 2003 r. do 7,5% w 2015 r.

[10] Stany: CA, IL, LA, MD, NH, NC, OR, TN, VA, WA.



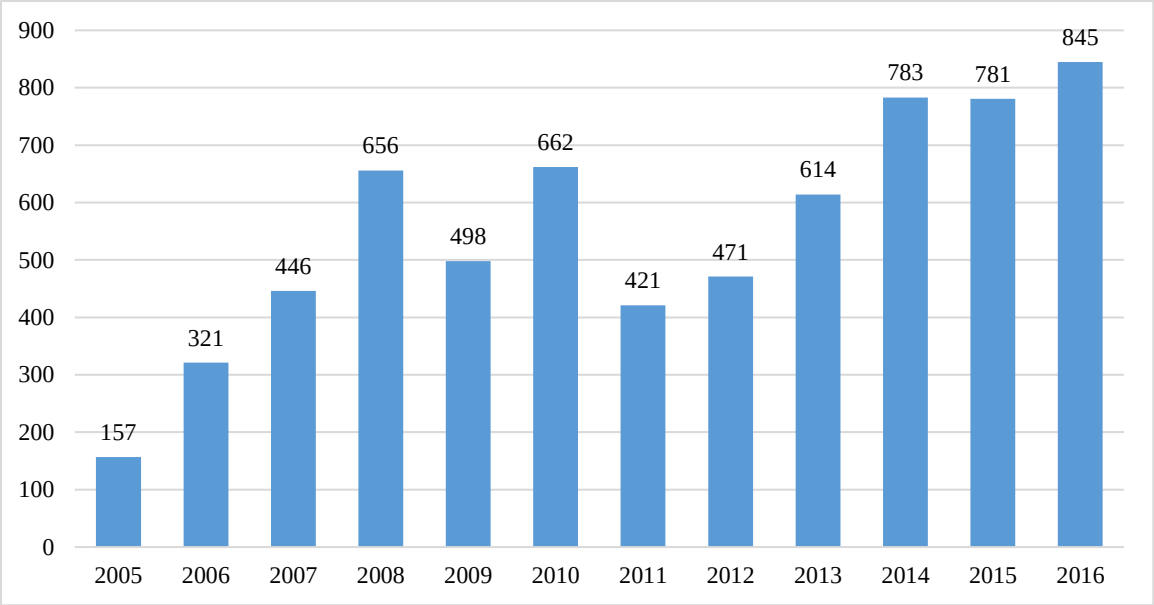
Rys. 1. Liczba stanów USA posiadających obowiązujące przepisy o obowiązku notyfikacji poszkodowanych w razie naruszenia bezpieczeństwa danych w latach 2003-2015 oraz wskaźnik penetracji ubezpieczeń cybernetycznych w USA (w %)
Źródło: [Ayers 2015].

W analizowanym okresie miał miejsce dynamiczny wzrost liczby zawartych umów ubezpieczenia cyber, czego wyrazem jest wysoki przeciętny wskaźnik wzrostu składki przypisanej brutto wynoszący około 32% (rys. 2). W 2015 r. na rynku amerykańskim przypis składki osiągnął 2,4 mld USD, natomiast według dostępnych prognoz w 2016 r. dojdzie do przekroczenia bariery 3 mld USD [Betterley 2016]. Na wynik ten złożył się nie tylko coraz większy popyt na ochronę cyber, ale również skokowy wzrost stawek ubezpieczeniowych w sezonie odnowieniowym 2016 r., spowodowany rosnącą szkodowością tej linii ubezpieczeń [Willis Towers Watson 2016].



Rys. 2. Przypis składki z cyber ubezpieczeń w USA w latach 2002-2016 (szacunkowo, w mln USD)
Źródło: opracowanie własne na podstawie [Betterley 2016].

Konsekwencją implementacji przepisów o ochronie danych osobowych w kolejnych stanach USA jest przyrost liczby ujawnionych wypadków naruszenia bezpieczeństwa danych. Jednym z prawdopodobnych efektów tych doniesień jest wzrost świadomości cyber zagrożeń i dostrzegania jego obecności w najbliższym otoczeniu. To z kolei stanowi bez wątpienia impuls stymulujący podjęcie decyzji o zakupie cyber ubezpieczenia. Wzmocnienie tego efektu następuje również wtedy, gdy media informują o wyjątkowo dużych, wręcz spektakularnych wydarzeniach polegających na wycieku danych wrażliwych. W samych Stanach Zjednoczonych dochodzi do nich kilkukrotnie w ciągu roku. Na rys. 3 przedstawiono liczbę ujawnionych *data breach* w latach 2005-2016 (dla 2016 r. stan na 1 XI). Ich liczba wskazuje na tendencję wzrostową, choć tempo przyrostów w ostatnich trzech latach wyhamowało w porównaniu z okresem 2005-2008 lub 2012-2014.

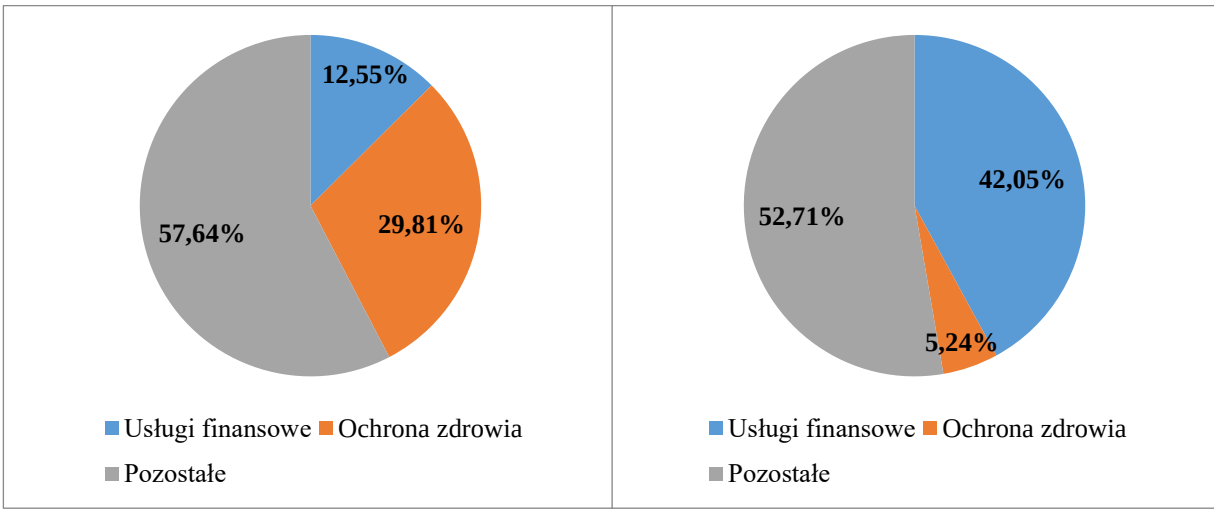


Rys. 3. Liczba ujawnionych *data breach* w USA (stan na dzień 20.11.2016)
Źródło: opracowanie własne na podstawie danych z Identity Theft Resource Center, www.idtheftcenter.org (dostęp 29.11.2016)

Doświadczenia amerykańskie pokazują, że liczba zgłoszonych wypadków naruszenia bezpieczeństwa danych wzrosła średnio o 75% w ciągu roku od wejścia w życie regulacji dotyczących obowiązku notyfikacji, zaś po upływie trzech lat od implementacji tych przepisów wzrost liczby powiadomień wyniósł średnio 150% [Ayers 2015]. Można zatem powiedzieć, iż efekty obowiązywania ustawodawstwa odnoszącego się do *data breach* ujawniają się już po krótkim czasie, ale stają się wyraźnie widoczne dopiero w perspektywie średnioterminowej. Wprowadzanie przepisów stanowych zaostrzających odpowiedzialność administratora za naruszenie ochrony danych osobowych w połączeniu ze wzrostem liczby incydentów raportowanych do wiadomości publicznej stanowi ważny czynnik wzrostu rynku cyber ubezpieczeń w USA, co potwierdzają dane o przypisie składki i penetracji rynku zaprezentowane powyżej.

Na poziomie prawa federalnego obowiązują ustawy HIPAA dla sektora ochrony zdrowia i ubezpieczeń zdrowotnych oraz Gramm-Leach-Bliley dotycząca instytucji finansowych. Na podstawie danych przedstawionych poniżej można sformułować tezę, iż te branże reprezentują wyższy popyt na ochronę ubezpieczeniową w zakresie cyber ryzyka, co wynika z obciążenia odpowiedzialnością wynikającą z regulacji HIPAA i GLBA. Ponad 40% udział w liczbie zgłoszonych incydentów typu *data breach* oraz blisko 50% udział w wolumenie bezprawnie ujawnionych rekordów danych świadczy o wysokim stopniu narażenia na ryzyko cybernetyczne (rys. 4). W raporcie badającym strukturę szkód zgłoszonych z ubezpieczeń cyber w USA wyraźnie widać dominację sektora ochrony zdrowia (19%

zgłoszonych szkód cybernetycznych), podczas gdy sektor instytucji finansowych uplasował się na czwartym miejscu (10%), tuż za przemysłem (13%) i branżą obsługującą gry i kasyna elektroniczne (11%) [Net Diligence 2016]. Ochrona zdrowia jest sektorem, w którym wskaźnik penetracji ubezpieczeń cyber jest najwyższy (41% podmiotów z tego sektora posiada cyber-polisę). Nieco niższy wynik osiągnęły instytucje finansowe (20%), choć z drugiej strony to właśnie w tym segmencie nabywców ubezpieczeń cyber przeciętne limity pokrycia są tradycyjnie najwyższe – 21,6 mln USD [Marsh 2015]. Ponadto, przeznaczając największą część swoich budżetów (szacunkowo 10-12%) na ochronę przed cyber zagrożeniami spośród wszystkich branż gospodarki, instytucje finansowe dywersyfikują katalog stosowanych narzędzi zarządzania cyber ryzykiem, przez co rola cyber ubezpieczeń w tym mixie jest relatywnie ograniczona [SANS 2016].



Rys. 4. Udział sektora usług finansowych i ochrony zdrowia w liczbie ujawnionych wypadków data breach (wykres lewy) i w liczbie ujawnionych rekordów danych (prawy wykres) w USA w latach 2005-2016
Źródło: opracowanie własne na podstawie danych z Privacy Rights Clearinghouse, www.privacyrights.org (dostęp 21.11.2016)

Zdaniem Schwartz i Janger [2006], nałożenie na podmiot, w którym doszło do wycieku danych, obowiązku notyfikacji wszystkich osób, których dane dotyczą, pod groźbą odpowiedzialności karnej w razie nie wywiązania się z niego, jest wyraźnym indykatorem kierunku przyjętej polityki legislacyjnej w odniesieniu do ochrony danych osobowych. Polega ona na wymuszeniu należytej staranności na administratorach danych osobowych poprzez zagrożenie wysokimi karami finansowymi i osądzeniem w postępowaniu karnym. Dodatkowo w części stanów, ustawodawca wyposażył poszkodowanych obywateli w prawo dochodzenia roszczeń odszkodowawczych w postępowaniu cywilnym z tytułu strat majątkowych spowodowanych nieautoryzowanym wykorzystaniem danych osobowych.

Należy wspomnieć, że prawo stanowe, w którym nie uzależnia się obowiązku notyfikacji od wcześniejszej analizy ryzyka wynikającego z wycieku danych osobowych (tzw. *harm threshold*), poddawane jest krytyce. Burdon i in. [2010] obawiają się deprecjacji znaczenia zawiadomień o naruszeniu bezpieczeństwa danych, które będą docierać do poszkodowanych osób ze zbyt dużą częstotliwością lub dotyczyć będą naruszeń nie stanowiących realnego zagrożenia. Postuluje się wprowadzenie odpowiednio wysokiego pułapu liczby ujawnionych danych, którego przekroczenie prowadziło by do powstania obowiązku notyfikacji. Do podobnych wniosków doszli Schwartz i Janger [2006].

Podsumowanie

Jeszcze do niedawna organizacja, która doświadczyła wycieku gromadzonych przez nią danych osobowych, mogła całkowicie ukryć ten fakt, gdyż nie było przepisów regulujących obowiązki informacyjne w razie incydentu naruszenia bezpieczeństwa informacji (*data breach*). W wielu krajach nawet uchwalenie odpowiednich aktów prawnych nie poprawiło sytuacji osób, których dane dotyczą, dlatego że nie przewidziano w nich powiadamiania wszystkich poszkodowanych, uznając za wystarczające zawiadomienie odpowiedniego regulatora (w Polsce jest to GIODO).

System ochrony danych osobowych w USA jest zdececentralizowany, gdyż składa się z dwóch poziomów – federalnego i stanowego. Prawo stanowe ma charakter ogólny, powszechny (tzn. dotyczy wszystkich branż gospodarki bez wyjątku) i skupia się na ochronie konsumenta poprzez obowiązkową notyfikację o wypadkach naruszenia prywatności oraz ograniczaniu rozmiarów strat w drodze stosowania odpowiednich polityk bezpieczeństwa informacji w organizacjach. Przepisy federalne odnoszą się natomiast do wybranych, konkretnych sektorów gospodarki (np. sektor usług finansowych, ubezpieczenia zdrowotne, systemy kart płatniczych).

Zwolnienie z obowiązku notyfikacji w przypadku wycieku danych w zakodowanej formie powinno zachęcać – zdaniem legislatorów – do wykorzystywania w administrowaniu danymi bezpiecznych technologii szyfrowania danych.

W niniejszej pracy wykazano wyraźny wpływ regulacji stanowych i federalnych wprowadzających obowiązek notyfikacji o wycieku danych na rozwój rynku ubezpieczeń cybernetycznych w USA. W związku z tym można oczekiwać, że implementacja podobnych

regulacji do prawodawstwa Wspólnotowego wywoła pozytywny efekt na europejski rynek cyber-ubezpieczeń, który obecnie znajduje się w początkowym stadium rozwoju.

Prezentowana praca ma charakter przyczynkowy do dyskusji o czynnikach determinujących popyt na ubezpieczenia cybernetyczne. Problematyka ta wymaga dalszych, pogłębionych badań teoretyczno-poznawczych, jaki i empirycznych – nie tylko rynku amerykańskiego, ale także europejskiego.

Bibliografia

Ayers E. [2015], *Federal data breach notification law seen as cost-saving measure*, Advisen, 27 marzec 2015, http://www.cyberrisknetwork.com/2015/03/27/federal-data-breach-notification-law-seen-cost-saving-measure/ (dostęp 12.11.2016)

Betterley [2016], *Cyber/privacy insurance market survey*, czerwiec 2016, https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf (dostęp 26.11.2016)

Burdon M., Lane B., von Nessen P. [2010], *The mandatory notification of data breaches: Issues arising for Australian and EU legal developments*, "Computer Law & Security Review", Vol. 26(2), s. 115-129.

Ecora [2016], *Practical guide to understanding and complying with the Gramm-Leach-Bliley Act*, http://www.ecora.com/Ecora/whitepapers/IDRS_GLBA.pdf (dostęp 22.11.2016)

Komisja Europejska [2010], *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z dnia 4 listopada 2010 r., KOM(2010) 609, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pl.pdf (dostęp 18.11.2016)

Krzysztofek M. [2014], *Ochrona danych osobowych w Unii Europejskiej*, Wyd. Wolters Kluwer, Warszawa.

Marsh [2015], *Benchmarking trends: Cyber-attacks drive insurance purchases for new and existing buyers*, October 2015, http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/US-en/Mid-Year%20Cyber%20Benchmarking%20Report-10-15.pdf (dostęp 2.12.2016)

Net Diligence [2016], *2016 Cyber claims study*, https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf (dostęp 12.09.2016)

SANS [2016], *IT security spending trends*, Instytut SANS, Luty 2016, https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697 (dostęp 30.11.2016)

Schwartz P.M., Janger E.J. [2006], *Notification of data security breaches*, „Michigan Law Review", Vol. 105, s. 915-984.

Smyth S.M. [2013], *Does Australia really need mandatory data breach notification laws – and if so, what kind?*, "Journal of Law, Information and Science", Vol. 22 (2), s. 159-169

Ustawa GLBA [1999], *Gramm-Leach-Bliley Act* z dnia 12 listopada 1999 r. (USA), Public Law 106-102, 113 Statute, ss. 1338-1481, https://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf (dostęp 11.10.2016)

WEF World Economic Forum [2016], *The global risks report 2016*, Insight Report, 11th edition, http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf (dostęp 23.09.2016)

Willis Towers Watson [2016], *Marketplace realities. 2016 Spring update*, http://www.willis.com/documents/publications/Industries/construction/MR%20Spring%20Update%20Final.pdf (dostęp 23.06.2016)