PO I Ds. 48.2020

POSTANOWIENIE

o umorzeniu dochodzenia

Gdańsk, dnia 19 kwietnia 2021 roku

Wojciech Chmielewski – prokurator Prokuratury Rejonowej Gdańsk-Oliwa w Gdańsku delegowany do Prokuratury Okręgowej w Gdańsku
po zapoznaniu się z aktami o sygnaturze PO I Ds. 48.2020
w sprawie uzyskania bez uprawnień w okresie od 15 kwietnia 2020 roku do 16 kwietnia 2020 roku w nieustalonym miejscu za pośrednictwem sieci Internet poprzez niezabezpieczony port serwera informacji dla niego nieprzeznaczonej w postaci bazy danych klientów firmy Fortum Marketing and Sales S.A.
to jest o czyn z art. 267§1 k.k..

na podstawie art. 17 § 1 pkt. 2 k.p.k.

postanowił:

umorzyć dochodzenie:

I. w sprawie uzyskania bez uprawnień w okresie od 15 kwietnia 2020 roku do 16 kwietnia 2020 roku w nieustalonym miejscu za pośrednictwem sieci Internet poprzez niezabezpieczony port serwera informacji dla niego nieprzeznaczonej w postaci bazy danych klientów firmy Fortum Marketing and Sales S.A.

tj. o czyn z art. 267§1 k.k. – wobec stwierdzenia, że czyn nie zawiera znamion czynu zabronionego /art. 17§1 pkt 2 k.p.k./

II. w sprawie przetwarzania, w nieustalonym w okresie od 12 kwietnia 2020 roku do 16 kwietnia 2020 roku w Gdańsku, danych osobowych klientów firmy Fortum Marketing and Sales S.A. chociaż ich przetwarzanie nie jest dopuszczalne lub bez uprawnienia

tj. o czyn z art. 107 ust 1 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych – wobec stwierdzenia, że czyn nie zawiera znamion czynu zabronionego /art. 17§1 pkt 2 k.p.k./

U z a s a d n i e n i e :

Prokuratura Okręgowa w Gdańsku pod sygnaturą akt PO I Ds. 48.2020 nadzorowała wszczęte w dniu 5 maja 2020 roku dochodzenie w sprawie uzyskania bez uprawnień w okresie od 15 kwietnia 2020 roku do 16 kwietnia 2020 roku w nieustalonym miejscu za pośrednictwem sieci Internet poprzez niezabezpieczony port serwera informacji dla niego nieprzeznaczonej w postaci bazy danych klientów firmy Fortum Marketing and Sales S.A. to jest o czyn z art. 267§1 k.k.. W toku postępowania ustalono co następuje.

W dniu 24 kwietnia 2020 roku Fortum Marketing and Sales Polska S.A. powiadomił tutejszą prokuraturę o możliwości popełnienia przestępstwa z art. 267§1 k.k. polegającego na uzyskaniu nieuprawnionego dostępu do informacji obejmujących dane osobowe klientów spółki. W uzasadnieniu wskazano, że zawiadamiający prowadzi działalność gospodarczą w zakresie obrotu energią elektryczną i paliwem gazowym, w tym w zakresie sprzedaży energii elektrycznej oraz gazu odbiorcom końcowym zarówno sektora biznesowego, jak i gospodarstwom domowym. W ramach prowadzonej działalności spółka Fortum współpracuje z PIKA Sp. z o.o. w Gdańsku. W oparciu o zawartą umowę PIKA świadczy na rzecz Fortum usługi różnego rodzaju, w tym usługę cyfrowego archiwum umów, jakie spółka Fortum zawarła z klientami. Pracownicy zawiadamiającego mają zdalny dostęp do cyfrowego, do którego dane osobowe klientów trafiają poprzez automatyczny skan dokumentów. Automatycznego skanowania dokumentów dokonuje PIKA. W następstwie zgłaszanych uwag dotyczących spowolnienia funkcjonowania cyfrowego archiwum, PIKA poinformowała w dniu 14 kwietnia 2020 roku, że utworzyła dodatkową wtórną i pomocniczą bazę metadanych o nazwie ElasticSearch (bez zasilenia jej obrazami skanów i bez komunikacji z głównym serwerem bazodanowym dla archiwum NUXEO). Pierwsze zasilenie danymi rzeczywistymi tej bazy nastąpiło 12 kwietnia 2020 roku począwszy od godziny 13:00 z zakończeniem ok. godziny 19:30. W dniu 16 kwietnia 2020 roku zawiadamiający stwierdził naruszenie bezpieczeństwa danych osobowych, które jest związane z faktem wprowadzania przez pracowników PIKA zmiany w środowisku teleinformatycznym dla usługi Nuxeo Fortum, której celem było zwiększenie wydajności działania całości archiwum cyfrowego. Z informacji otrzymanych od operatora usługi chmurowej – Beyond.pl Sp. z o.o. w Poznaniu (działającego na zlecenie PIKA) wynika, że do skopiowania danych doszło w nocy z 15 na 16 kwietnia 2020 roku w godzinach 23:00-04:00. Stwierdzono również, iż baza danych ElasticSearch nie była odpowiednio zabezpieczona. Informację o naruszeniu

bezpieczeństwa danych osobowych Fortum otrzymało drogą elektroniczną z dwóch niezależnych źródeł (VolodymyrDiachenko i Michała Brygidyna). Niezwłocznie po uzyskaniu informacji baza została wyłączona. Hasła dostępowe do systemów i środowisk zostały zmienione. Zawiadamiający wskazał, iż baza danych obejmowała rekordy dotyczące 137 tysięcy klientów spółki Fortum Marketing and Sales Polska S.A.. Pozostawione na serwerze dane dotyczyły zawartych umów sprzedaży energii elektrycznej i paliwa gazowego. Obejmowały między innymi imię, nazwisko, adres, numer telefonu, PESEL i/lub numer dowodu osobistego.

Przesłuchany w charakterze świadka Krzysztof Dziewirz specjalista IT w Fortum Marketing and Sales Polska S.A. zeznał, że w dniu 16 kwietnia 2020 roku zostali powiadomieni przez Volodymyra Diachenko oraz Michała Brygidyn o możliwości swobodnego dostępu do niezabezpieczonej bazy danych klientów spółki Fortum, przechowywanej w systemie Fortum Nuxeo. Świadek zeznał, że system ten spełnia rolę archiwum cyfrowego dokumentów i informacji na temat klientów. W okresie naruszenia, czyli ekspozycji niezabezpieczonej bazy danych o nazwie ElasticSearch w systemie NUXEO, czyli od 12 kwietnia 2020 roku od godziny 12:00 do 16 kwietnia 2020 roku do godziny 11:57, stwierdzono wyłącznie dwa incydenty związane z jej skopiowaniem. Na podstawie analizy danych połączeń z serwera świadek wskazał, że do skopiowania bazy danych mogło dojść wyłącznie w okresie od 15 kwietnia 2020 roku od godziny 19:22 do dnia 16 kwietnia 2020 roku godzina 04:06. Poza tymi dwoma incydentami dochodziło wyłączenie do okazjonalnych połączeń z bazą ElasticSearch, które w ocenie administratora były wyłączenie połączeniami o charakterze skanów penetracyjnych, a nie kopiowania danych. Charakterystyczne połączenia wskazujące na kopiowanie zawartości danych miały miejsce z dwóch adresów IP. Pierwsze z tych połączeń wykonano w dniu 15 kwietnia 2020 roku w godzinach 19:22-20:58. Skopiowano wówczas plik o rozmiarze około 5MB. Drugie połączenie miało miejsce w dniu 15 kwietnia 2020 roku od godziny 23:00 do dnia 16 kwietnia 2020 roku do godziny 04:06. Wówczas mogło dojść do pobrania danych w wolumenie około 11 GB.

Świadek Tomasz Majewski z PIKA Sp. z o.o. zeznał, że na zlecenie Fortum Marketing and Sales Polska S.A. współtworzył system elektronicznego obiegu informacji pozyskanych z digitalizacji dokumentów. W związku z problemami dotyczącymi powolnego wyszukiwania danych w bazie głównej na zlecenie klienta wdrożono funkcjonalność pozwalającą na przyśpieszenie operacji wyszukiwania danych poprzez umieszczenie kluczowych indeksów w bazie pomocniczej ElasticSearch. Funkcjonalność ta jest opcjonalnym dodatkiem w postaci modułu dodawanego na życzenie klienta do systemu elektronicznego obiegu dokumentów o nazwie NUXEO. System działał na serwerach dzierżawionych od firmy Beyond. W projekcie oprócz świadka brali udział także Marcin Czajkowski, Maciej Stępniak i Bartosz Lizak. Za pomysł i wykonanie projektu odpowiedzialny był Bartosz Lizak, który

przekazał do wykonania zadanie działowi utrzymywania,w ramach którego za przygotowanie środowiska do pracy bazy ElasticSearch odpowiedzialny był Marcin Czajkowski. Tenże stworzył na serwerze firmy Beyond nowy wirtualny serwer, na którym zainstalowano ElasticSearch. Podczas instalacji nie zwrócono jednak uwagi, że serwer stworzony przez Marcina Czajkowskiego nie został zabezpieczony. Baza została zasilona danymi w dniu 12 kwietnia 2020 roku. W wytycznych projektu nie wskazano jednoznacznie jak powinna wyglądać komunikacja z bazą oraz jakie powinny zostać użyte zabezpieczenia. Jednakże w ocenie świadka, Marcin Czajkowski jako inżynier i specjalista od systemów powinien o to zadbać albowiem wiedział czego dotyczy projekt i co ma się znajdować w bazie. Takie zabezpieczenia uchodzą za standardową praktykę. Marcin Czajkowski stworzył projekt według wytycznych ale nie zabezpieczył komunikacji. Stworzone środowisko nie zostało także zweryfikowane przez zespół świadka pod kątem bezpieczeństwa. W wyniku tego błędu baza danych klientów spółki Fortum Marketing and Sales Polska była ogólnie dostępna w okresie od 12 do 16 kwietnia 2020 roku. Z posiadanej przez świadka wiedzy wynika, że doszło wyłącznie do dwóch skutecznych logowań do bazy danych zakończonych pobraniem pakietów danych. Jedno z pobrań było niewielkie, zaś drugie z dużym prawdopodobieństwem doprowadziło do skopiowania całej bazy danych.

Powyższe okoliczności potwierdzili także Bartosz Lizak i Maciej Stępniak. Maciej Czajkowski przyznał, że utworzył wirtualny serwer nie zabezpieczając go. Wskazał jednak, że nie otrzymał takiego polecenia i nie miał świadomości do czego serwer miał służyć.

W toku śledztwa przesłuchano również osoby, które ujawniły istnienie niezabezpieczonego serwera z danymi oraz powiadomiły o tym administratora danych.

Michał Brygidyn zeznał, że w dniu 15 kwietnia 2020 roku około godziny 21:00 korzystając z wyszukiwarki shodan.io z filtrem kraju na Polskę, odnalazł niezabezpieczony serwer ElasticSearch. Świadek postanowił zidentyfikować właściciela serwera i przy użyciu wtyczki do przeglądarki o nazwie elasticsearch head wykonał czynności zmierzające do „odpytywania" serwera. Sprawdził także ilość dokumentów oraz próbkę testową, w celu potwierdzenia co się tam znajduje. Nie pobierał ani nie kopiował ujawnionych danych. Jedyny transfer jaki wykonał mógł wynikać z podglądu danych na przeglądarce w celu ustalenia właściciela i potwierdzenia autentyczności. Dane przeglądał pomiędzy godziną 21:00, a 21:30. Potem niezwłocznie wysłał wiadomość na adres rodo@fortum.com informując o wycieku danych, ale nie otrzymał informacji zwrotnej. Kolejnego dnia ponownie skontaktował się poprzez portal Linked In z Prezesem Zarządu spółki Fortum informując o zdarzeniu. W trakcie ujawnienia bazy danych świadek korzystał z usługi NordVPN i nie zna adresu IP z jakiego łączył się z serwerem. Podejrzewa jednak, że będzie to adres IP z terenu Polski.

Przesłuchany w drodze międzynarodowej pomocy prawnej na Ukrainie – Volodymyr Diachenko zeznał, że jest przedsiębiorcą pracującym w segmencie cyberbezpieczeństwa w firmach i przedsiębiorstwach, które popełniły błędy w konfiguracji ustawień baz danych. Częścią jego pracy jest badanie wykorzystywania wyszukiwarek publicznych oraz analiza ich zawartości w celu zapobiegawczym. Często pracuje z własnej inicjatywy wykorzystując systemy poszukiwania (Google i Shodan). W dniu 16 kwietnia 2020 roku około 01:00 czasu obowiązującego w Kijowie (02:00 czasu polskiego), podczas wyszukiwania w systemie Shodan świadek ujawnił niezabezpieczoną bazę danych, która podczas dalszej analizy okazała się być częścią infrastruktury chmury firmy Fortum Marketing ans Sales Polska S.A.. O ujawnionym niezabezpieczonym porcie niezwłocznie powiadomił drogą elektroniczną zarząd niniejszej spółki. Nie logował się serwer albowiem został on nieprawidłowo skonfigurowany. Każdy mógł na niego wejść. Świadek nie pobierał danych z serwera ale przeglądał go w czasie rzeczywistym. Wszelkie dane pobrane do analizy świadek zniszczył.

W toku postępowania dokonano zabezpieczenia serwera na którym umieszczoną bazę ElasticSearch oraz poddano ją badaniom przez biegłych z zakresu informatyki. W opinii biegłych do udostępnienia (pobrania) danych doszło poprzez nieuprawniony zdalny dostęp do zasobów serwerowych przez otwarty port 9200/TCP w infrastrukturze PIKA Sp. z o.o.. Udostępnienie danych zawierających dane klientów podmiotu Fortum Marketing and Sales Polska S.A. lub uzyskanie dostępu do takich danych było wynikiem umożliwienia ich pobrania przez otwarty port 9200/TCP zarządzany w ramach infrastruktury PIKA. Biegli nie ustalili treści pobranych danych. W ocenie biegłych, uwzględniając dane przekazane przez PIKA Sp. z o.o. ujawnieniu poddano 26,2 GB danych. Wskazane dane pobrano jednokrotnie z ustalonego adresu IP przypisanego do miasta Kijów na Ukrainie. Dostęp do wskazanych zasobów został również uzyskany z innych adresów, jednak ujawnione transfery danych były niewielkie. Z kolejnego pod kątem wielkości pobrania danych adresu IP pobrano łączenie 15,97 MB danych, zaś z pozostałych 3 adresów IP nie więcej niż 462 KB.

Zestawiając wyniki analizy biegły z podjętymi w sprawie ustaleniami wskazać należy, iż jedyne duże pobranie bazy danych odpowiada adresowi IP, z którego otwarty serwer danych weryfikował Volodymyr Diachenko. Pobraniu temu odpowiada także czas, w jakim świadek dokonywał zapoznania się z danymi w nocy z 15 na 16 kwietnia 2020 roku. Drugie połącznie skutkujące pobraniem pakietu danych o pojemności 15,97 MB odnotowano z adresu IP przypisanego do Dublina. Nie można zatem wykluczyć, iż odpowiada on adresowi IP użytkowanemu w usłudze NordVPN, przez Michała Brygidin. W tym wypadku również przemawia za tym czasokres, w którym Michał Brygidin dokonywał analizy tego serwera i bazy danych. Pozostałe pobrane pakiety danych były znikome co pozwala z dużą dozą prawdopodobieństwa założyć, iż jak wskazał świadek Krzysztof Dziewirz - specjalista IT w Fortum Marketing and Sales Polska S.A., miały one charakter penetracyjny i nie skutkowały

pobraniem danych. Dlatego też można założyć, iż mimo pozostawienia niezabezpieczonej bazy danych, nie doszło do jej pobrania i późniejszego rozpowszechnienia (poza pobraniem danych przez Michała Brygidyn i Volodymyra Diachenko, którzy według swoich deklaracji, po analizie pakiety te zniszczyli).

Analizując zgromadzony w sprawie materiał dowodowy wskazać należy, iż będący przedmiotem postępowania czyn nie wyczerpuje znamion czynu zabronionego.

Występek z art. 267§1 k.k. popełnia ten, kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Z literalnego brzmienia przepisu wynika wprost, iż do realizacji znamion czynu zabronionego dojdzie wyłącznie wówczas, gdy łącznie zostaną spełnione dwie przesłanki. Pierwsza polega uzyskaniu możliwości dostępu do informacji nieprzeznaczonej dla danego odbiorcy. Druga przesłanka wskazuje zaś na określony sposób uzyskania niniejszego dostępu, który polegać musi na podłączeniu do sieci informatycznej albo na działaniu polegającym na przełamaniu lub ominięciu zabezpieczeń. Uzyskanie dostępu do informacji musi bowiem nastąpić bez uprawnienia, czyli mieć charakter nielegalny, naruszający prawo innego podmiotu do dysponowania informacją czy też jej uzyskiwania (por. Mozgawa M. (red.), Budyn-Kulik M., Kozłowska-Kalisz P., Kulik M., Kodeks karny. Komentarz aktualizowany, LEX/el., 2021).

W okolicznościach niniejszego postępowania bezspornym jest, że pierwsza z dwóch przesłanek zaistniała. Nie ulega bowiem wątpliwości, iż baza klientów spółki Fortum Marketing and Sales Polska nie stanowiła informacji publicznej dostępnej dla nieograniczonego kręgu osób. Wręcz przeciwne, z uwagi na specyfikę tych danych oraz zawarte w nich dane osobowe, w tym numery PESEL, a nawet dane dowodu osobistego, numer telefonu czy adres, dane te winny być szczególnie chronione przed ich udostępnieniem lub rozpowszechnieniem. Nie była to zatem informacja przeznaczona dla otwartego katalogu odbiorców.

Zupełnie odmiennie przedstawia się natomiast sytuacja z drugą z wymienionych przesłanek. Czyn zabroniony popełnia bowiem jedynie ten, kto dostęp do informacji dla niego nie przeznaczonej uzyskuje otwierając zamknięte pismo, albo podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Ustawodawca wyróżnił zatem trzy sytuacje, które wymagają analizy w niniejszym postępowaniu. Pierwsza polega na otwarciu zamkniętego pisma; druga na podłączeniu się do sieci telekomunikacyjnej, zaś trzecia na podjęciu działań zmierzających do złamania lub obejścia zabezpieczeń sieci telekomunikacyjnej.

Pierwszy przypadek należy zdecydowanie odrzucić. W okolicznościach niniejszej sprawy, baza danych klientów Fortum Marketing and Sales Polska S.A. miała formę elektroniczną, zaś zgromadzone tak dane przechowywane były na serwerze. Nie doszło zatem do uzyskaniu dostępu do danych poprzez otwarcie zamkniętego pisma.

Dwa kolejne przypadki wiążą się z funkcjonowaniem sieci telekomunikacyjnej, której definicja zawarta została w art. 2 pkt 35 ustawy z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Dz.U. z 2021, poz. 576). Zgodnie z przywołanym przepisem sieć telekomunikacyjną stanowią systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju. Bezspornym jest zatem, iż serwery służące do przechowywania danych, w tym bazy klientów użytkującego ją podmiotu, są częścią sieci telekomunikacyjnej. Dlatego też podłączenie się do takiego serwera (sieci telekomunikacyjnej) lub też przełamanie czy obejście jego zabezpieczeń stanowi czyn zabroniony z art. 267§1 k.k..

Podłączenie do sieci telekomunikacyjnej zostaje zrealizowane poprzez podłączenie urządzenia odbiorczego do sieci kablowej (telefonicznej, komputerowej) lub innej infrastruktury (optycznego, radiowego czy w inny sposób wykorzystującej energię elektromagnetyczną) służącej do przekazywania informacji. Podłączenie może dotyczyć zarówno sieci przewodowej, jak i bezprzewodowej. W literaturze prawa karnego trafnie wyróżnia się jednak trzy sytuacje. „Po pierwsze, może zdarzyć się tak, że osoba uzyska dostęp do sieci otwartej. W tym wypadku z oczywistych względów nie dojdzie do realizacji znamion, każda osoba jest bowiem jej potencjalnym uprawnionym użytkownikiem. Po drugie, sprawca może podłączyć się do sieci w sposób nieuprawniony, w wyniku czego uzyska możliwość przesyłania i odbierania informacji, co do których jest uprawniony. Dochodzi tutaj jedynie do nieuprawnionego wykorzystania urządzenia przesyłowego. Zachowanie takie także nie stanowi czynu przestępnego – czyn sprawcy nie odnosi się bowiem w ogóle do jakiejkolwiek informacji o charakterze poufnym, pozostając poza zakresem ochrony normy. Po trzecie – podłączenie się do sieci może wiązać się z uzyskaniem dostępu do określonych danych, udostępnionych wyłącznie jej użytkownikom (np. na dysku sieciowym) i objętych ochroną art. 267. Jeśli sprawca uzyskuje do nich dostęp w wyniku podłączenia się do sieci, jego zachowanie może realizować znamiona przestępstwa" (por. Wróbel W. (red.), Zoll A. (red.), Barczak-Oplustil A., Bielski M., Bogdan G., Ćwiąkalski Z., Iwański M., Jodłowski J., Kardas P., Małecki M., Pilch A., Raglewski J., Rams M., Sroka T., Szewczyk M., Wojtaszczyk A., Zając D., Zontek W., Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d, WKP, 2017).

Z perspektywy rozpatrywanej sprawy najistotniejsze znaczenie ma pierwsza z przywołanych sytuacji. Podłączenie się do otwartej sieci telekomunikacyjnej, nie może bowiem stanowić czynu zabronionego z art. 267§1 k.k., nawet wówczas, gdy umożliwia zapoznanie się z informacjami nie przeznaczonymi dla podłączającego. W dobie ogólnej cyfryzacji i wszechobecnego Internetu, trudno uznać za przestępcze, zachowania polegające na przeszukiwaniu sieci w celu ujawnienia określonych informacji. Obecnie każdy człowiek posiadający dostęp do Internetu wpisując w wyszukiwarce określone hasło lub adres IP, może uzyskać połączenie z dowolnym serwerem („chmurą") zawierającym określone informację, których szuka. O ile zatem serwery te nie są zabezpieczone przez powszechnym dostępem, nie sposób przypisać komuś karnych konsekwencji zapoznania się z informacjami na nich umieszczonymi oraz uznawać takie podłączenie do sieci telekomunikacyjnej za nielegalne.

Podobnie ocenić sytuację, gdy wskazane dane zostały umieszczone na serwerze, ale poprzez błąd ludzki, nie zostały one zabezpieczone przed ich udostępnianiem. W doktrynie trafnie przyjmuje się, że „jeżeli sprawca wykorzystuje błąd programisty i wchodzi do systemu przez "dziurę" w konfiguracji lub oprogramowaniu systemowym po to, by uzyskać znajdującą się w systemie informację, to nie można mu nawet przypisać usiłowania przestępstwa, o którym mowa w art. 267 § 1 k.k.. Jeżeli "przechodzenie przez dziurę" nie wymaga od hackera ingerencji w zapis na komputerowym nośniku informacji lub korzystania ze specjalnego oprogramowania, zachowanie takie w ogóle nie jest karalne" (por. Adamski Andrzej, Karalność hackingu na podstawie przepisów kodeksu karnego z 1997 r., PS.1998.11-12.149). „Nie popełnia przestępstwa z art. 267 § 1 k.k. osoba uzyskująca nieuprawniony dostęp do informacji bez przełamania lub ominięcia zabezpieczenia, nawet jeśli zrobi to podstępem" (por. wyrok SA w Szczecinie z 14.10.2008 r., II AKa 120/08, LEX nr 508308 [w] Konarska-Wrzosek V. (red.), Lach A., Lachowski J., Oczkowski T., Zgoliński I., Ziółkowska A., Kodeks karny. Komentarz, WKP 2020).

Zatem uzyskanie informacji, co do której nie przedsięwzięto żadnych środków ochronnych, nie stanowi przestępstwa z art. 267 § 1 k.k., chyba że polega na „nielegalnym" (podkreś. wł.) podłączeniu się do sieci telekomunikacyjnej (por. Mozgawa M. (red.), Budyn-Kulik M., Kozłowska-Kalisz P., Kulik M.Kodeks karny. Komentarz aktualizowanyLEX/el., 2021; Wróbel W. (red.), Zoll A. (red.), Barczak-Oplustil A., Bielski M., Bogdan G., Ćwiąkalski Z., Iwański M., Jodłowski J., Kardas P., Małecki M., Pilch A., Raglewski J., Rams M., Sroka T., Szewczyk M., Wojtaszczyk A., Zając D., Zontek W., Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d, WKP, 2017).

W okoliczności niniejszego postępowania tak się właśnie stało. Dane personalne klientów Fortum Marketing and Sale Polska S.A. poprzez błąd ludzki zostały pozostawione na niezabezpieczonym serwerze danych, skąd zostały dwukrotnie skutecznie pobrane przez

Michała Brygidyn i Volodymyra Diachenko. Niezwłoczna reakcja tychże dwóch osób i powiadomienie właściciela danych o ich wycieku, uchroniło wskazane informacje przed dalszym skutecznym pobieraniem z serwera i następczym rozpowszechnianiem. Dlatego też nie sposób uznać, że w niniejszym postępowaniu doszło do bezprawnego, w rozumieniu art. 267§1 k.k., podłączenia się do sieci telekomunikacyjnej lub podjęciu działań zmierzających do przełamania lub ominięcia takiej sieci. Powodem udostępniania danych był wyłącznie błąd ludzki, który nie wyczerpał znamion czynu zabronionego z art. 267§1 k.k., zaś może ewentualnie rodzić odpowiedzialnością cywilną lub administracyjną.

Obowiązujące z Unii Europejskiej przepisy dotyczące ochrony danych osobowych, w tym rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO), choć szeroko regulują zasady postępowania z danymi osobowymi, nie zawierają żadnych rozstrzygnięć w zakresie sankcji karnych za ich złamanie. W preambule przywołanego rozporządzenia wskazano, że państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie tego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Ich zakres i kształt pozostawiono jednak poszczególnym państwom członkowskim.

Obowiązująca do dnia 6 lutego 2019 roku ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2016, pozycja 922 t.j.), obejmowała przepisami karnoprawnymi między innymi umyślne i nieumyślne udostępnianie danych osobom nieuprawnionym przez tego, kto administruje zbiorem danych lub jest obowiązany do ochrony danych osobowych (art. 51), a także umyślne i nieumyślne naruszanie przez osobę administrującą danymi, obowiązku zabezpieczenia tych danych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem (art. 52). Wskazane przepisy z chwilą wejścia w życie ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. z 2019 roku, poz. 1781 t.j.) zostały jednak uchylone. Ustawodawca przyjmując nową ustawę dopasowaną do nowych regulacji europejskich (RODO), znacząco zmniejszył ilość czynów karalnych wskazując, że jego celem było ograniczenie przepisów karnych do niezbędnego z punktu widzenia systemu ochrony danych osobowych minimum i przeniesienie ciężaru reakcji karnej na prawo administracyjne i administracyjne kary pieniężne.

Obowiązująca od 2018 roku ustawa o ochronie danych osobowych przewiduje sankcje karne wyłącznie za przetwarzanie danych osobowych, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania dana osoba nie jest uprawniona (art. 107 ust 1 ustawy), z wyższą sankcją karną w przypadku przetwarzania danych wrażliwych (art. 107 ust 2 ustawy), a także za udaremnienie lub utrudnianie kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych (art. 108 ustawy).

Mając na uwadze powyższe uznano, że czyny polegające na pozostawieniu w okresie od 12 do 16 kwietnia 2020 roku na niezabezpieczonym serwerze danych 137.000 klientów Fortum Marketing and Sale Polska S.A., przez administratora tychże danych, jak również uzyskanie bez uprawnień w okresie od 15 kwietnia 2020 roku do 16 kwietnia 2020 roku w nieustalonym miejscu za pośrednictwem sieci Internet poprzez niezabezpieczony port serwera informacji dla niego nieprzeznaczonej w postaci bazy danych klientów firmy Fortum Marketing and Sales S.A. nie wyczerpywały znamion czynu zabronionego.

W toku postępowania podjęto również czynności zmierzające do zbadania uprawnień Fortum Marketing and Sales Polska S.A do przetwarzania danych swoich klientów przez pryzmat art. 107 ust 1 ustawy o ochronie danych osobowych. Do złożonego przez Fortum Marketing and Sales Polska S.A. zawiadomienia o popełnieniu przestępstwa z art. 267§1 k.k. przystąpiło bowiem wielu klientów spółki, zaś kilkunastu z nich wskazywało także, że spółka nie miała uprawnień do przetwarzania ich danych albowiem klienci ci skutecznie wypowiedzieli umowy oraz złożyli wnioski o usunięcie ich danych z bazy.

Wskazać należy, iż zgodnie z przywołanym już wyżej rozporządzeniem Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) (CELEX 32016R0679), przetwarzanie danych jest zgodne z prawek wyłącznie w przypadkach, gdy spełniony został jeden z warunków określonych w art. 6 ust 1 lit. a – f. Do przesłanek tych należą miedzy innymi sytuację gdy:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; I

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Spółka Fortum Marketing and Sale Polska uzasadniając przechowywanie danych klientów, z którymi związana była umowami, nawet po ich rozwiązaniu lub wypowiedzeniu wskazała, że przetwarza dane osobowe klientów niezbędne do zawarcia i realizacji umowy i przez okres niezbędny do realizacji celu przetwarzania, czyli przez czas trwania umowy (art. 6 ust. 1 lit. b RODO) oraz na podstawie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f RODO) przez czas przedawnienia roszczeń, a także w oparciu o obowiązek przechowywania niektórych danych na podstawie przepisów prawa (art. 6 ust. 1 lit. c RODO). Wskazała nadto, że dane osobowe klientów mogą zostać usunięte po zakończeniu okresu obowiązywania zawartej umowy, przedłużonego o okres, w którym możliwe jest dochodzenie roszczeń w związku z tą umową (okres retencji danych), nie później jednak niż po upływie 6 lat od zakończenia obowiązywania umowy. W okresie retencji dane te są przetwarzane wyłącznie w celu dochodzenia ewentualnych roszczeń lub obrony przed nimi. Fortum Marketing and Sales Polska wskazała również, że osobnym przypadkiem jest sytuacja kiedy klient korzysta z prawa do odstąpienia od umowy. W przypadku skutecznego odstąpienia od umowy, podstawą przetwarzania staje się uzasadniony interes administratora danych związany z przeprocesowaniem odstąpienia. Fortum jako administrator danych ustaliło okres 3 miesięcy jako czas niezbędny do przeprocesowania odstąpienia tj. połączenia dokumentu odstąpienia z odpowiednią umową oraz weryfikacji skuteczności odstąpienia. Po tym okresie dane osobowe w systemach Fortum są anonimizowane (co jest równoznaczne z ich usunięciem). Dane osobowe klientów zanonimizowane w systemach Fortum, pozostają jednak w archiwum prowadzonym przez Podmiot Przetwarzający (PIKA Sp. z o.o.), gdzie przetwarzane są wyłącznie w celach archiwalnych i statystycznych zgodnie z art. 89 ust. 1 RODO w zw. z art. 5 ust. 1 lit e RODO. Dane te będą systematycznie usuwane i ostateczny termin ich usunięcia był zaplanowany na koniec 2020 roku, jednakże w związku z postępowaniem toczącym się przed Prezesem Urzędu Ochrony Danych Osobowych, związanym z wyciekiem danych, usuwanie tych danych zostało wstrzymane. Zawiadamiający wskazał nadto, że nie przetwarza danych osobowych klientów na podstawie zgody (art. 6 ust. 1 lit. a RODO), a co za tym idzie nie mogą oni wycofać zgody na przetwarzanie danych osobowych (ponieważ jej nie udzielali). Wnioski o usunięcie danych osobowych są procesowane zgodnie z przepisami RODO i realizowane wtedy kiedy wygasły wszystkie podstawy prawne do ich przetwarzania.

Przenosząc powyższe okoliczności na grunt rozpatrywanej sprawy ponownie wskazać należy, iż nowa ustawa o ochronie danych osobowych nie powiela przepisów RODO, lecz uzupełnia nowe regulacje w zakresie ochrony danych osobowych, tak aby odpowiadały przepisom i standardom przyjętym na poziomie Unii Europejskiej. Przepisy ustawy stanowią jedynie dopełnienie RODO, w zakresie w jakim ustawodawca unijny dopuścił doprecyzowanie pewnych zagadnień, na porządek prawny w państwach

członkowskich, w tym w zakresie odpowiedzialności karnej. Odpowiedzialność karna ma być co do zasady wyjątkiem przewidzianym dla najcięższych naruszeń przepisów i stanowić jedynie uzupełnienie dla odpowiedzialności administracyjnej oraz cywilnej. W uzasadnieniu ustawy wskazano, iż odpowiedzialność karna powinna mieć charakter wyjątkowy i odnosić się do najpoważniejszych naruszeń przepisów. (por. M.Zimna, Odpowiedzialność karna za naruszenie ochrony danych osobowych, Prokuratura i Prawo, 2020, nr 1, str. 63).

Zgodnie z art. 107 ust 1 ustawy o ochronie danych osobowych kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega karze. W myśl cytowanego przepisu odpowiedzialności karnej podlega zatem wyłącznie ten kto przetwarza dane gdy nie jest to dopuszczalne lub nie jest do tego uprawniony. Przetwarzanie nie jest natomiast dopuszczalne gdy nie zachodzi żadna z przesłanek wymienionych w art. 6 RODO.

Mając natomiast na uwadze, iż w okolicznościach niniejszego postępowania wskazane przesłanki z art. 6 RODO istniały, nie sposób przyjąć, że przetwarzanie danych klientów Fortum Marketing and Sales Polska S.A. w celu zagwarantowania realizacji umowy oraz na podstawie uzasadnionego interesu administratora przez okres przedawnienia roszczeń, wyczerpywało znamiona czynu zabronionego. Tym bardziej w sytuacji, gdy zgodnie z założeniami ustawy oraz RODO, sankcja karna ma mieć charakter subsydiarny wobec kar o charakterze administracyjnym lub cywilnym. Analogicznie należy ocenić także znamię podmiotu uprawnionego do przetwarzania danych. Spółka Fortum jako strona umowy z klientami miała bowiem uzasadniony interes i prawo, aby takie dane przetwarzać.

Mając na uwadze powyższe okoliczności postanowiono jak w sentencji postanowienia.

PROKURATOR PROKURATORY REJONOWEJ
Delegowany do Prokuratury Okręgowej
Wojciech Chmielewski

Pouczenie:
1. Na powyższe postanowienie przysługuje zażalenie do sądu właściwego do rozpoznania sprawy (art. 306 § 1a k.p.k., oraz art. 465 § 2 k.p.k.):
- stronom procesowym,
- instytucji państwowej lub samorządowej, która złożyła zawiadomienie o przestępstwie,
- osobie, która złożyła zawiadomienie o przestępstwie określonym w art. 228-231, art. 233, art. 235, art. 236, art. 245, art. 270-277, art. 278-294 lub w art. 296-306 Kodeksu karnego, jeżeli postępowanie karne wszczęto w wyniku jej zawiadomienia, a wskutek tego przestępstwa doszło do naruszenia jej praw.

Sąd może utrzymać w mocy zaskarżone postanowienie lub uchylić je i przekazać sprawę prokuratorowi celem wyjaśnienia wskazanych okoliczności bądź przeprowadzenia wskazanych czynności (art. 330 § 1 k.p.k.).
Jeżeli prokurator nadal nie znajdzie podstaw do wniesienia aktu oskarżenia wyda ponownie postanowienie o odmowie wszczęcia śledztwa – dochodzenia*) lub o jego umorzeniu. Postanowienie to podlega zaskarżeniu tylko do prokuratora nadrzędnego. W razie utrzymania w mocy zaskarżonego postanowienia pokrzywdzony, który dwukrotnie wykorzystał uprawnienia przewidziane w art. 306 § 1 i 1a, może wnieść akt oskarżenia określony w art. 55 § 1 k.p.k. W takim przypadku akt oskarżenia do sądu wnosi się w terminie miesiąca od daty doręczenia zawiadomienia o postanowieniu prokuratora nadrzędnego o utrzymaniu w mocy zaskarżonego postanowienia,

dołączając po jednym odpisie dla każdego oskarżonego oraz dla prokuratora (art. 330 § 2 k.p.k., art. 55 § 1 k.p.k.). Akt oskarżenia winien spełniać wymogi określone w art. 55 § 1 i 2 k.p.k.
Inny pokrzywdzony tym samym czynem może aż do rozpoczęcia przewodu sądowego na rozprawie głównej przyłączyć się do postępowania (art. 55 § 3 k.p.k.).
2. Uprawnionym do złożenia zażalenia, o którym mowa w art. 306 § 1a k.p.k., przysługuje prawo przejrzenia akt sprawy (art. 306 § 1b k.p.k.).
3. Na postanowienie co do dowodów rzeczowych zażalenie przysługuje stronom oraz osobie, od której odebrano przedmioty lub która zgłosiła do nich roszczenie (art. 323 § 2 k.p.k.).
4. Zażalenie wnosi się za pośrednictwem prokuratora, który wydał postanowienie. Termin do wniesienia zażalenia wynosi 7 dni od daty doręczenia odpisu postanowienia i jest zawity. Zażalenie wniesione po upływie tego terminu jest bezskuteczne (art. 122 § 1 i 2, art. 460 k.p.k.).

Zarządzenie:

Stosownie do treści art. 305§4 k.p.k. i art. 131§3 i 4 k.p.k. odpis postanowienia zamieścić na stronie internetowej Prokuratury Okręgowej w Gdańsku.