

X kadencja



# KANCELARIA SEJMU

## Biuro Komisji Sejmowych

### **PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA**

- **KOMISJI CYFRYZACJI, INNOWACYJNOŚCI  
I NOWOCZESNYCH TECHNOLOGII  
(NR 131)  
z dnia 3 września 2026 r.**



---

# Pełny zapis przebiegu posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 131)

3 września 2026 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Bartłomieja Pejo (Konfederacja)**, przewodniczącego Komisji, rozpatrzyła:

– **informację na temat bezpieczeństwa danych medycznych pacjentów w systemach cyfrowych na przykładzie wycieku danych z platformy MyDr.**

W posiedzeniu udział wzięli: **Michał Gramatyka** sekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Tomasz Maciejewski** podsekretarz stanu w Ministerstwie Zdrowia wraz ze współpracownikami, **Jacek Młotkiewicz** dyrektor Departamentu Kontroli i Naruszeń Urzędu Ochrony Danych Osobowych wraz z współpracownikami, **Michał Mamica** zastępca dyrektora Departamentu Bezpieczeństwa Urzędu Komunikacji Elektronicznej wraz ze współpracownikiem, **Maciej Siciarek** kierownik Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, **Jeremi Olechnowicz** dyrektor Pionu Eksploatacji Systemów Teleinformatycznych (ZDIII) Centrum e-Zdrowia, **Mariusz Siemiradzki** członek zarządu Krajowej Izby Komunikacji Ethernetowej, **Albert Szczepaniak** członek Rady Legislacyjnej Związku Pracodawców Polska Chmura wraz ze współpracownikami, **Joanna Karczewska** członek Stowarzyszenia Absolwentów Elektroniki na Politechnice Warszawskiej @ELKAPW oraz **Marika Kowalska** członkini Forum STEM.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Magdalena Krzymowska** i **Jakub Konecki** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

## **Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dzień dobry. Bardzo serdecznie witam wszystkich państwa.

Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, stwierdzając jednocześnie kworum.

Witam bardzo serdecznie panie i panów posłów.

Witam serdecznie pana ministra Michała Gramatykę, sekretarza stanu w Ministerstwie Cyfryzacji. Bardzo serdecznie witam pana ministra Tomasza Maciejewskiego, podsekretarza stanu w Ministerstwie Zdrowia, wraz ze współpracownikami. Witam przedstawicieli Urzędu Ochrony Danych Osobowych, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Centrum e-Zdrowia oraz Urzędu Komunikacji Elektronicznej. Serdecznie witam również reprezentację strony społecznej: Konfederację Lewiatan, Krajową Izbę Komunikacji Ethernetowej, Związku Pracodawców Polska Chmura, Forum STEM oraz Stowarzyszenia @ELKAPw. Witam serdecznie wszystkich państwa.

Porządek dzisiejszego posiedzenia przewiduje rozpatrzenie informacji ministra cyfryzacji oraz ministra zdrowia na temat bezpieczeństwa danych medycznych pacjentów w systemach cyfrowych na przykładzie wycieku danych z platformy MyDr.

Czy są uwagi do porządku obrad? Nie widzę. Przechodzimy zatem do jego realizacji.

Szanowni państwo, słowem wstępu. Tak jak mówi temat naszego dzisiejszego posiedzenia, opinia społeczna, posłowie – myślę, że wszyscy tutaj zgromadzeni, ale nie tylko tutaj – chcieliby usłyszeć od przedstawicieli ministerstw, jak chronione są dane medyczne, jak to wygląda na dzień dzisiejszy, jakie działania zostały podjęte po informacji o wycieku danych kilkunastu milionów obywateli. Chcemy się od państwa dowiedzieć tego i wiele więcej na przykładzie, tak zatytułowaliśmy, wycieku danych z platformy MyDr. To jest tylko przykład.

Jak w ogóle są chronione dane pacjentów w Polsce? Co więcej w tym temacie możecie państwo zrobić jako przedstawiciele ministerstw, ale również co my możemy zrobić jako parlamentarzyści? Jeśli mamy jakąś możliwość pomocy, to oczywiście jesteśmy do dyspozycji jako przedstawiciele

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. W tym temacie chcielibyśmy dzisiaj szeroko i konkretnie porozmawiać.

Bardzo proszę o zabranie głosu pana ministra Michała Gramatykę. Proszę bardzo.

**Sekretarz stanu w Ministerstwie Cyfryzacji Michał Gramatyka:**

Bardzo dziękuję. Bardzo dziękuję za zwołanie tego posiedzenia Komisji, za poświęcenie go tematowi, które są dość wrażliwe, dość sensytywne, a jak nasze doświadczenia pokazują – również dość aktualne.

W zasadzie wiele powiedziano na temat tego przestępstwa na szkodę prywatnej firmy, do którego doszło w drugiej połowie sierpnia. Prywatna firma, która koncentrowała u siebie dane kilkunastu milionów Polaków, wykonywała oprogramowanie dla około 12 tys. placówek medycznych. Najczęściej to było oprogramowanie typu elektroniczna dokumentacja medyczna (EDM), czyli takie systemy kompleksowego zarządzania. Po prostu sprzedawała to oprogramowanie placówkom medycznym. Zostaliśmy poinformowani, że firma ta padła ofiarą ataku i że w wyniku ataku istnieje niebezpieczeństwo, że z archiwów firmy gromadzone przez nią dane mogły trafić w niepowołane ręce. Ministerstwo Cyfryzacji, Naukowa i Akademicka Sieć Komputerowa, wszyscy odpowiedzialni za tego typu incydenty natychmiast podjęli działania. Te działania były obliczone głównie na to, żeby sprawdzić, czy ta informacja jest prawdziwa, czy są jakieś elementy, które pozwalają zweryfikować taką informację.

W tym cyfrowym świecie jest dokładnie tak jak w świecie analogowym. Tak jak w analogowym świecie zdarzają się włamania, na przykład do mieszkań czy do domów, różne rzeczy giną, tak w świecie cyfrowym od czasu do czasu zdarzają się włamania do systemów IT i wykradane są dane. Powszechna cyfryzacja sprzyja zwiększeniu się liczby prób czy incydentów – tak to nazywamy. To są incydenty w zakresie cyberbezpieczeństwa. Polski system cyberbezpieczeństwa jest zorganizowany w taki sposób, że w cywilnej części codziennie dostajemy informacje, ile było podejmowanych takich prób ataków, w jaki sposób te dane... To znaczy, jaka jest dynamika tych danych, czy tych prób jest więcej, z mniej więcej jakim wektorem one wychodzą.

W omawianym przypadku sprawcy tego przestępstwa rozpoczęli korespondencję z jednym z fachowych dziennikarzy zajmujących się problematyką cyberbezpieczeństwa poprzez odpowiednik portalu społecznościowego posadowiony na tzw. sieci fediverse, na powiedzmy, że takiej sieci opensource'owej, otwartej. To jest dość niszowe środowisko. W każdym razie udało się nam zweryfikować, że ta informacja o wycieku jest prawdziwa. Udało się to zweryfikować za pomocą paczki danych dostarczonych przez włamywaczy, przez przestępców. W związku z tym zostały podjęte działania przez wyspecjalizowane jednostki Policji, zostało wszczęte postępowanie w prokuraturze i zaczęliśmy podejmować wszystkie te działania, które powinny zostać podjęte w wypadku takich właśnie wydarzeń. Ostatnim etapem czy ostatnim aktem tych działań póki co było umieszczenie w portalu bezpieczne dane.gov.pl – to jest jeszcze dzieło naszych poprzedników – informacji o tym, czyje numery PESEL padły czy mogły paść ofiarą przestępstwa.

Na dzień dzisiejszy jest prowadzony stały monitoring tych rubieży internetu, które są wykorzystywane przez przestępców na okoliczność tego, czy te dane w jakikolwiek sposób są udostępnione, czy ktoś na przykład składa ofertę handlu tymi danymi, czy też te dane pojawiają się gdzieś w darknecie, w undernecie, we wszystkich tych przestrzeniach. Ten monitoring daje wynik negatywny. Co więcej, sami sprawcy, a przynajmniej osoby, które przyznają się do popełnienia tego włamania w korespondencji ze wspomnianym dziennikarzem – co zresztą państwo mogą znaleźć na mediach społecznościowych, dlatego że te komunikaty są tam publikowane – takim dość charakterystycznym językiem próbują powiedzieć, że celem ich działania nie było to, żeby te dane w jakikolwiek sposób udostępniać, tylko testowanie odporności systemów informatycznych.

Od strony czysto profesjonalnej prowadzone jest postępowanie, prowadzone są czynności policyjne. To, co mogliśmy zrobić, to zachęcamy wszem i wobec ludzi do zastrzegania numerów PESEL. Baza danych, numerów PESEL osób, które mogły być dotknięte – podkreślam to, mogły być dotknięte – tym przestępstwem została udostępniona w serwisie bezpieczne dane.gov.pl. Stworzyliśmy też system kolejkowania ze względu na to, że każdy, kto się loguje do tego systemu, obciąża węzeł krajowy, czyli węzeł, którym autoryzujemy się wszyscy do usług państwowych. Za pomocą systemu kolejkowania zabezpieczyliśmy więc ten system, żeby po prostu nie wyrzucił w powietrze, żeby nie zawiesił węzła krajowego. Ponad 2 mln Polaków sprawdziło te numery PESEL. Dość powszechnie mówi się w zasadzie we wszystkich publikacjach o konieczności zastrzegania numeru PESEL.

Jednocześnie przygotowaliśmy projekt ustawy. We współpracy z osobami odpowiedzialnymi za ochronę danych osobowych przygotowaliśmy projekt regulacji, który zabezpieczy nas na przyszłość, dlatego że przyczyną tej sytuacji, przyczyną tego przestępstwa była zbyt duża koncentracja danych w jednym miejscu. To zbyt duża koncentracja danych w jednym miejscu jest dla nas wyzwaniem na przyszłość. Stąd pojawił się pomysł tzw. cyber piątki, czyli pięciu wymogów, które mają spowodować, że na przyszłość tego typu sytuacje będą lepiej zabezpieczone.

Po pierwsze, wymóg odpowiedniej certyfikacji w zakresie cyberbezpieczeństwa firm, które świadczą takie usługi, które mogą koncentrować dane więcej niż 100 tys. Polek i Polaków. Po drugie, zwiększenie wytycznych technologicznych związanych z bezpieczeństwem systemu, gdzie te dane są przetwarzane. Jest to większa przejrzystość. Chcemy doprowadzić do sytuacji, w której osoba, która mogła paść ofiarą takiego ataku, będzie pozyskiwała nie tylko prostą informację. Na dzisiaj jest to informacja, że jej PESEL brał udział w tym zdarzeniu, że jej PESEL stał się łupem przestępców – żadnej innej informacji. Chcemy, żeby na przyszłość takie osoby dostawały bardzo precyzyjne informacje, jakie dane mogły paść ofiarą tych przestępców.

Chcemy również legislacyjnie doprowadzić do sytuacji, żeby dostawać powiadomienia o takich sytuacjach poprzez państwowe aplikacje – to znaczy poprzez mObywatela i poprzez Internetowe Konto Pacjenta – zarówno te związane z przejęciem danych, jak i te, w których ktokolwiek będzie się usiłował posłużyć tymi danymi. To jest w zasadzie wszystko, co możemy zrobić. Tam, gdzie mamy do czynienia z danymi cyfrowymi, tam, gdzie mamy do czynienia z systemami IT, tego typu sytuacje... Nie chcę mówić, że one są codziennością, ale one co jakiś czas się zdarzają.

Nie dalej jak kilka lat temu rozmawialiśmy o gigantycznym wycieku, który dotknął jedną z największych polskich firm diagnostycznych. Nie dalej jak kilka lat temu rozmawialiśmy o międzynarodowym wycieku, którego ofiarą padł jeden z największych systemów bankowych, powszechnie używany w Stanach Zjednoczonych, ale nie tylko w Stanach Zjednoczonych. Był to międzynarodowy bank, duża korporacja. Co jakiś czas dostają państwo informacje od platform e-commerce, w których robią państwo zakupy internetowe, że w wyniku incydentu cyberbezpieczeństwa mogło dojść do ujawnienia takich a takich danych, prosimy o zwrócenie szczególnej uwagi, prosimy o zastrzeżenie numeru PESEL, o zmianę hasła. Takie sytuacje się zdarzają.

Od strony czysto legalnej instytucjami, które są odpowiedzialne za informowanie swoich klientów, są instytucje końcowe. Ta prywatna firma, która została dotknięta przestępstwem, nie była administratorem danych, ona była jedynie podmiotem, który przetwarzał te dane. Warto też wspomnieć, że te dane to są dane archiwalne. To są dane, których aktualność kończy się chyba na końcu roku 2024.

#### **Głos z sali:**

W kwietniu.

#### **Sekretarz stanu w MC Michał Gramatyka:**

W kwietniu 2024 r. Więc wszyscy ci, których dane mogły paść ofiarą przestępców, powinni zostać poinformowani przez przychodnie, przez placówki medyczne, w których mogli wykonywać badania. Wiemy, że część z tych placówek medycznych już przekazuje takie informacje.

Pytanie pana przewodniczącego dotyczące danych państwowych, danych w systemach, w rejestrach państwowych, danych zdrowotnych Polaków gromadzonych w tych rejestrach państwowych to jest pytanie o tyle słuszne, co zasługujące na odpowiedź, że te dane są bezpieczne. Tak jak odnotowujemy setki prób zaatakowania systemów państwowych, tak nie odnotowaliśmy nigdy skutecznej próby. Dane państwowe były, są i będą bezpieczne.

Przyjmowaliśmy nie tak dawno ustawę o krajowym systemie cyberbezpieczeństwa, która jest takim zestawem narzędzi prawnych dotyczących cyberbezpieczeństwa. Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii opiniowała i prowadziła bardzo szczegółową pracę nad tą ustawą, więc wydaje się, że ten legalny przyborek, ustawa podpisana przez pana prezydenta, dość dobrze nas zabezpiecza.

To, o czym warto pamiętać i to, co my możemy zrobić, to jest w zasadzie niewiele więcej oprócz zastrzeżenia PESEL. Pocieszającą informacją jest informacja, że tych danych nigdzie nie ma. Te dane nie zostały wystawione na sprzedaż. Nikt nie używa tych danych do szantażu. Osoby, które przeczesują internet w poszukiwaniu tej gigantycznej paczki danych, bo to są terabajty danych, nie odnalazły żadnego śladu wskazującego na to, żeby te dane trafiły do domeny publicznej.

To w zasadzie tyle tytułem wstępu. Oczywiście mamy przygotowany materiał. Ja przepraszam, jestem w zastępstwie za kolegę.

Nie wiem, czy materiał już został do państwa wysłany, czy dopiero zostanie. OK, ale nie mamy problemu z tym, żeby go państwu przekazać. Dlatego pozwoliłem sobie omówić go dość szczegółowo.

Jesteśmy do dyspozycji w bardzo mocnym gronie ekspertów. Nie mówię o sobie, tylko o osobach reprezentujących Centrum e-Zdrowie, Naukową i Akademicką Sieć Komputerową oraz Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji. W razie gdyby pojawiły się pytania, na które ja nie będę w stanie odpowiedzieć, to poproszę prawdziwych fachowców. Dziękuję.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję, panie ministrze.

Zanim będą pytania i dyskusja, to chętnie posłuchamy wypowiedzi pana ministra Tomasza Maciejewskiego, któremu już za moment oddam głos. Natomiast tradycyjnie dziękuję za mocną, merytoryczną obecność państwa na w zasadzie wszystkich posiedzeniach Komisji.

Panie ministrze, bardzo proszę o zabranie głosu.

**Podsekretarz stanu w Ministerstwie Zdrowia Tomasz Maciejewski:**

Panie przewodniczący, szanowni państwo, ważna informacja jest taka, że w ramach tego incydentu nie doszło do naruszenia centralnego systemu e-zdrowie platformy P1. Wszystkie usługi centralne cały czas funkcjonowały i funkcjonują. Nie odnotowaliśmy żadnych krytycznych ani niekrytycznych incydentów w tym zakresie. Tak jak powiedziałem, dane, które są w systemach publicznych, tak jak powiedział pan minister, są nadal bezpieczne.

Od razu po ujawnieniu tego incydentu włączyliśmy się we współpracę. Departament zdrowia i nasz sektorowy zespół cyberbezpieczeństwa dla ochrony zdrowia (CSIRT CeZ) Centrum e-Zdrowia włączył się do współpracy ze swoimi odpowiednikami w Ministerstwie Cyfryzacji. Naszym pierwszym zadaniem było zweryfikowanie, czy nie doszło do naruszenia naszej platformy P1.

Druga rzecz – przystąpiliśmy do weryfikacji certyfikatów, które są używane do komunikacji między jednostkami ochrony zdrowia a naszą platformą P1. Następnie włączyliśmy proces wymiany tych certyfikatów w sposób uporządkowany, oczywiście skoordynowany. Chodziło o to, aby wyłączyć z ruchu certyfikaty, w przypadku których mogła istnieć szansa, że są skompromitowane. To jest dość prosty proces. On jest znany użytkownikom. Każdy z użytkowników systemu, który kontaktuje się z systemem P1, musi wymieniać taki certyfikat co trzy lata, więc nie jest to żadna nowość. Zostały one wymienione w celach prewencyjnych, po to żeby nie doszło do jakiegokolwiek możliwości ataku.

Jednocześnie zwróciliśmy się też z informacją i z prośbą do Zakładu Ubezpieczeń Społecznych, aby również on wymienił ich certyfikaty u tych podmiotów, które używały aplikacji MyDr i żeby ich personel medyczny też wymienił swoje certyfikaty ZUS-owskie, aby się zabezpieczyć. To są działania prewencyjne. Nie wystąpiły żadne naruszenia w systemach ZUS ani w naszym systemie P1. Tym niemniej te klucze są pewnymi kluczami do wejścia do systemu.

Tych systemów nie zamknęto. Oczywiście nie włączono tych kluczy jednego dnia, bo sparaliżowałoby to funkcjonowanie systemu ochrony zdrowia. Zostało to wykonane etapami. Wszyscy w tym czasie mogli korzystać z systemu, tak że dla użytkowników, dla każdego z nas jako pacjenta ten proces przebiegł tak naprawdę w sposób niezauważalny. Jednocześnie zostały wydane zalecenia do wszystkich podmiotów, które były wskazane w ramach tego incydentu do weryfikacji swoich systemów, do wymiany certyfikatów, jak również wdrożenia wszelkich zaleceń i sprawdzenia swoich procedur cyberbezpieczeństwa.

Ten proces oczywiście cały czas się toczy. Cały czas jesteśmy w procesie, bo działania instytucji nadzorujących ten incydent nadal trwają. Jeżeli pojawią się jakieś nowe informacje, to oczywiście, że będziemy państwu je przekazywać na bieżąco. Na dzień dzisiejszy nie odnotowaliśmy żadnego z problemów w zakresie publicznych systemów ochrony zdrowia. Nie doszło do naruszeń, wycieków. Można powiedzieć, że na dzień dzisiejszy na razie nie zgłaszamy problemów. Dziękuję bardzo.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję, panie ministrze.

Pozwolę sobie wprowadzić w temat, to znaczy w kwestię pytań. Mamy zatem pytanie.

W moim przekonaniu panowie mówicie o tym, że dane w tej chwili przechowywane w systemach są bezpieczne. Jednak okazuje się, że nie były bezpieczne przynajmniej do momentu tego

wycieku, kiedy 19 mln danych w jakiś sposób wyciekło. Natomiast pytanie brzmi, czy wiemy, jaka jest skala wycieku. W sensie nie ilość danych, tylko ich zakres. Nie chodzi o liczbę obywateli, których dane wyciekły, a o sam zakres tego, co wyciekło. Czy to są właśnie tylko imię, nazwisko, PESEL, czy również jakieś dane medyczne, recepty i inne dane wrażliwe tego typu?

Kolejne pytanie. Podejrzewam, że znam odpowiedź. Portal bezpiecznedane.gov.pl nie działał, kiedy osobiście wpisywałem swój PESEL kilka dni po wycieku. Zapewne był przeciążony. To jest też pytanie do państwa, dlaczego nie działał i jak długo nie działał. Dzisiaj działa. Przed chwilą sprawdzaliśmy.

Kolejne pytanie. Jakie są wnioski z tej sytuacji? Państwo wskazujecie na to, że to jest firma prywatna. Natomiast w moim przekonaniu firma prywatna powinna być w jakikolwiek sposób audytowana. Czy była audytowana? Jak wygląda bezpieczeństwo, ochrona tych danych przez instytucje państwowe, nawet jeżeli te dane posiada firma prywatna? Czy jest tu jakiejkolwiek współdziałanie z różnego rodzaju instytucjami i służbami, które mogłyby bardziej chronić te dane niż dotychczas?

To jest kilka pytań ode mnie na tę chwilę.

Czy teraz odpowiadamy? Tak będzie najlepiej.

Bardzo proszę, panie ministrze.

### **Sekretarz stanu w MC Michał Gramatyka:**

Pozwolę sobie zacząć od końca. Tak, to przestępstwo dotyczyło firmy prywatnej.

Na podstawie przepisów ustawy o krajowym systemie cyberbezpieczeństwa mamy taki rejestr podmiotów kluczowych i podmiotów ważnych. Ten rejestr jest uzupełniany na podstawie deklaracji. Gdyby ustawa o krajowym systemie cyberbezpieczeństwa już obowiązywała... Jesteśmy teraz w okresie przejściowym, a gdyby ta ustawa już obowiązywała w pełnym zakresie, to wszystko wskazuje na to, że producent oprogramowania, któremu skradziono te dane, byłby traktowany jak taki podmiot, a co za tym idzie – miałby dodatkowe obowiązki dotyczące utrzymania poziomu cyberbezpieczeństwa swoich systemów informatycznych.

Na początku, kiedy ta informacja trafiła do opinii publicznej, rzeczywiście któryś z członków kierownictwa Ministerstwa Cyfryzacji powiedział, że będziemy robić wszystko, żeby te dane jak najszybciej pojawiły się w systemie bezpiecznedane.gov.pl. Naturalnie w ten sposób została przetestowana odporność systemu na zwiększone zainteresowanie ze strony opinii publicznej, bo wszyscy nagle zaczęli się logować. Paradoksalnie wtedy tych danych zaimportowanych do systemu jeszcze nie było. Żeby te dane zaimportować, potrzebne było bowiem postanowienie prokuratury, która prowadzi śledztwo, więc nauczani doświadczeniem stworzyliśmy system kolejowania. W momencie, kiedy te dane rzeczywiście tam się pojawiły – to stało się, zdaje się, tydzień temu – wszyscy trafiali do kolejki. Po mniej więcej minucie, czasem dziewięćdziesięciu sekundach oczekiwania, dostawali dostęp do informacji o swoim numerze PESEL. To jest to, o co pan przewodniczący pytał – działania podjęte na przyszłość. Podjęliśmy na przykład takie działania.

Co jeszcze zrobiliśmy? Zakres danych, które padły ofiarą przestępców, znają dwa rodzaje podmiotów. Powinna go znać firma, która padła ofiarą przestępstwa, MyDr. Oni wiedzą, co wyciekło, są w stanie to zidentyfikować. Komunikacja z tą firmą jest dość trudna, dlatego że prowadzone tam są rozliczne kontrole, w szczególności przez Urząd Ochrony Danych Osobowych. Dostęp do tych danych powinny mieć również podmioty, na rzecz których to oprogramowanie powstawało, te podmioty, które są zgodnie z RODO zobowiązane do informowania swoich klientów, że dane wyciekły. To od nich klienci powinni dostawać konkretne informacje.

Legislacja, którą tworzymy, polega na tym, że zawsze wtedy, kiedy państwo posiada taką informację, będzie mogło przekazać taką informację obywatelom. Czyli jak gdyby wyprzedzamy tę sytuację poprzez systemy państwowe, poprzez mObywatela, poprzez Internetowe Konto Pacjenta, żeby po prostu przekazać w niezbędnym zakresie, jakie dane mogły paść ofiarom przestępców, ewentualnie poinformować Polki i Polaków, gdyby ktoś chciał użyć tych danych.

To by chyba było na tyle, jeśli chodzi o pytania zadane przez pana przewodniczącego. Mam nadzieję, żadnego nie zapomniałem, żadne mi nie uciekło. Bardzo dziękuję.

### **Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję. Tylko dopytam. Przecież te informacje o samym fakcie pozyskania, wycieku tych danych możemy sprawdzić na portalu bezpiecznedane.gov.pl, jak już działa. W takim razie, dlaczego... Zresztą nie wszyscy obywatele wiedzą o tym portalu. Moje pytanie brzmi: Dlaczego jako państwo nie możemy już teraz o tym poinformować, skoro jako państwo mamy te dane,

o wycieku konkretnych danych konkretnych osób? Chociażby nie wiem, przez mObywatela, SMS-owo, jakkolwiek inaczej: „państwa dane wyciekły”. Nie mówię o zakresie, tylko w ogóle o fakcie.

**Sekretarz stanu w MC Michał Gramatyka:**

Ale właśnie informujemy. System bezpiecznedane.gov.pl został zasilony tą zabezpieczoną przez cyberpolicję bazą danych PESEL. W komunikacji firmy, która padła ofiarą przestępstwa, czyli w komunikacji MyDr, pojawiają się takie wątki, że oni wcale nie mają pewności, czy wszystkie z tych numerów PESEL wyciekły, ale to jest działanie raczej podejmowane na zapas. Policja zabezpieczyła dane, zasiła tymi danymi portal bezpiecznedane.gov.pl. i to jest ścieżka, w oparciu o którą można powiadomić ludzi, czyli można ich zachęcić do tego, żeby sprawdzili swoje dane.

Podkreślam to, co mówię od początku. Te dane nie zostały skradzione z państwowych rejestrów. Państwo nie jest administratorem tych danych. Administratorem tych danych jest plus minus około 12 tys. podmiotów medycznych. To na nich ciąży obowiązek wynikający z RODO, czyli ustawy o ochronie danych osobowych. To przestępstwo dotknęło podmiot, który też nie jest administratorem tych danych. To jest podmiot przetwarzający te dane. Rzeczywiście ze względu na koncentrację dużej liczby tych danych... Jeżeli przyjmujemy nasze dodatkowe legislacje, jeżeli zacznie działać ustawa o krajowym systemie cyberbezpieczeństwa, to ten podmiot z mocy prawa będzie miał dodatkowe obowiązki, ale to prywatne podmioty mają ten obowiązek informowania. Państwo rzeczywiście wyszło naprzeciw temu. System bezpiecznedane.gov.pl, który m.in. został po to stworzony, zasililiśmy w taki sposób, żeby pokazały się w nim numery PESEL ludzi, którzy mogą się liczyć z wpływem czy z kradzieżą ich danych.

Pan przewodniczący jeszcze pytał o zakres tych danych. Z próbki przesłanej przez przestępców do portalu Zaufana Trzecia Strona, który był pierwszą jednostką informującą o tym całym fakcie, wynikało, że te dane mogą dotyczyć procedur medycznych i recept wypisywanych na poszczególne numery PESEL, natomiast pełny zakres tych danych znają tylko końcowi klienci firmy MyDr. To znaczy placówki medyczne, które kupowały u nich oprogramowania. Tylko oni wiedzą, w jaki sposób, jakimi danymi zasilali to oprogramowanie.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Tak, dziękuję, panie ministrze, tylko mnie dziwi to, że państwo jako państwo polskie, różnego rodzaju instytucje posiadające wiedzę o wpływie tych danych nie są w stanie zweryfikować czy pozyskać tych danych. Służby, Policja, jakkolwiek instytucje, które powinny się tym zajmować, w moim przekonaniu powinny natychmiast uzyskać informacje o zakresie danych i pozyskać je właśnie od tych podmiotów, które posiadają te dane. To po pierwsze.

Po drugie, pan minister mówi o KSC i że to mogłoby działać, gdyby KSC funkcjonowało w pełni, ale pytanie brzmiało, czy do tej pory w ogóle firma MyDr była jakkolwiek audytowana. Czy bezpieczeństwo tych danych w jakikolwiek sposób było kontrolowane przez państwo? Myślę, że to jest podstawa. Na tę chwilę z pana wypowiedzi wnioskuję, rozumiem, że... Dopóki nie działa KSC, to co? Każda prywatna firma może sobie robić cokolwiek – jakkolwiek zabezpieczyć albo nie zabezpieczyć danych medycznych pacjentów?

**Sekretarz stanu w MC Michał Gramatyka:**

Dość trudno jest udzielić jednoznacznej odpowiedzi na to pytanie. Ta sytuacja pokazuje, że rzeczywiście musimy podjąć działania legislacyjne zmierzające do wzrostu bezpieczeństwa danych. Jest pięć propozycji, które przedstawił pan premier Gawkowski, proponując... To jest pięć propozycji, nad którymi już pracujemy.

Jest to dodatkowa certyfikacja takich firm, które przetwarzają, koncentrują dużą ilość danych, dodatkowe wymogi dotyczące cyberbezpieczeństwa. Wychodząc naprzeciw pytaniom pana przewodniczącego, jest to obowiązek przekazywania całej informacji o tym, co padło ofiarą przestępców, do serwisu bezpiecznedane.gov.pl i obowiązek bezpośredniego informowania przez Internetowe Konto Pacjenta i przez mObywatela. Takie założenia, takie inicjatywy legislacyjne już są podjęte. Rząd już nad tym pracuje. Nadamy temu szybką ścieżkę, żeby te sprawy zostały uchwalone jak najszybciej.

Jeżeli chodzi o dane medyczne, to, zdaje się, w 2016 r. rząd podjął decyzję, że dopuszcza podmioty prywatne do tego obiegu, czyli do tworzenia systemów obsługujących placówki zdrowotne. Te podmioty prywatne odpowiadają za te dane. One odpowiadają wobec swoich klientów,

ale odpowiadają też wobec ludzi. To nie jest jedyna taka sytuacja. Podmioty prywatne na przykład agregują dane dzieci, które chodzą do szkół. Całe te systemy...

Była duża dyskusja na temat dziennika elektronicznego, ustawy, która została zawetowana przez pana prezydenta. To jest wypisz wymaluj taka sama sytuacja, tyle że tam nie ma danych medycznych, ale są wszystkie dane dotyczące wszystkich polskich uczniów i uczennic. One w zasadzie też są w rękach dwóch prywatnych korporacji, z których jedna jest amerykańska, druga jest transnarodowa. Takich sytuacji jest bardzo dużo. Wrażliwe dane bardzo często są w rękach podmiotów prywatnych. Wszystkie dane bankowe państwa są w rękach prywatnych podmiotów funkcjonujących w systemach bankowych. One oczywiście są bardzo wysoko regulowane i nad tym czuwają wszystkie państwowe urzędy, ale nie zmienia to faktu, że te dane są w rękach prywatnych. Więc takich sytuacji jest wiele.

Możemy brać odpowiedzialność za te dane, które są w posiadaniu państwa, za te, które są pomieszczone w systemach państwowych. One są zabezpieczone. W momencie, kiedy nasza legislacja przejdzie, podniesiemy również poziom bezpieczeństwa takich firm, które agregują u siebie więcej niż 100 tys. rekordów czy więcej niż 100 tys. zapisów związanych z jedną osobą. Myślę, że to jest dość racjonalny próg bezpieczeństwa.

Zwracam uwagę, że historycznie dotychczas kilka razy się zdarzało, że wyciekały dane medyczne, najczęściej z jednostek dużych laboratoriów diagnostycznych. Tutaj też mamy taką konkurencję na rynku, że mamy dwie albo trzy takie wielkie jednostki, które prowadzą diagnostykę. Tam też dochodziło do przestępstw, do ataków typu ransomware. Te dane były wystawiane na sprzedaż, żądano okupu od firm, więc to nie jest pierwsza tego typu sytuacja.

Natomiast ta sytuacja rzeczywiście jest dość poważna, bo przestępcy mówią o 18 mln rekordów. To jest bardzo dużo. To jest połowa całego społeczeństwa. Stąd nasze inicjatywy legislacyjne.

#### **Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję. Bardzo dobrze, że te inicjatywy są. Natomiast pan minister wprost nie odpowiedział na to pytanie, ale jak rozumiem i chyba wszyscy słyszymy, do momentu wprowadzenia KSC państwo polskie nie ma możliwości ochrony danych medycznych w posiadaniu firm prywatnych.

Żeby była jasność, absolutnie nie jestem przeciwnikiem działalności firm prywatnych. Wręcz przeciwnie – te firmy prywatne mogłyby funkcjonować tak, jak funkcjonują, tylko rolą państwa powinna być kontrola bezpieczeństwa tychże danych. Do momentu wdrożenia KSC, jak rozumiem, w zasadzie nie mamy najmniejszego wpływu na bezpieczeństwo tych danych i jako państwo polskie nie mamy kontroli nad danymi posiadanymi przez podmioty prywatne.

Panie ministrze, jeszcze mam jedną uwagę odnośnie do serwisu bezpiecznedane.gov.pl. Rozumiem, że każdy obywatel może sprawdzić, czy te dane wyciekły albo mogły wyciec, natomiast moja, nie wiem, sugestia czy uwaga jest taka, żeby poinformować tych wszystkich, osoby posiadające PESEL w tejże bazie danych bezpiecznedane.gov.pl, na przykład za pomocą mObywatela albo w jakikolwiek inny sposób: „Proszę pana, proszę pani, pani dane znajdują się w bazie bezpiecznedane.gov.pl, co oznacza, że mogły ulec wyciekowi”.

#### **Sekretarz stanu w MC Michał Gramatyka:**

Tak, ja też chciałbym, żeby tak było, natomiast w obecnym brzmieniu przepisów prawnych nie mamy podstawy prawnej do tego, żeby przekazać taką informację. Nie jesteśmy administratorem tych danych. Administratorem tych danych jest około 12 tys. placówek medycznych. One mają taki obowiązek. Państwo nie ma tytułu prawnego, żeby przekazać taką informację. I tak dość mocno się gimnastykowaliśmy, żeby w ogóle zaimportować te dane do bezpiecznedane.gov.pl.

To w ogóle jest paradoksalna sytuacja. Dość długo czekaliśmy na postanowienie prokuratora, które było dla nas tytułem prawnym do przekazania takiej informacji. Technicznie byliśmy gotowi do tego od razu. Natomiast dość długo trwało, zanim prokurator prowadzący śledztwo podjął taką decyzję, która w ogóle umożliwiła nam to informowanie. Wyprzedzając legislację, którą przygotowaliśmy... Ona będzie nam dawała taki tytuł zarówno do poinformowania w serwisie bezpiecznedane.gov.pl, jak i do przekazania takich informacji indywidualnie. Uważam, że rola państwa będzie zabezpieczona.

Nawiązując jeszcze do KSC, zostało ono uchwalone dość niedawno. Jesteśmy w okresie przejściowym. To jest bardzo duże osiągnięcie – dostosowanie polskiego prawa do wymogów dyrektywy NIS2. To cała ustawa o krajowym systemie cyberbezpieczeństwa. Tak, na pewno wszyscy pamiętamy, jak długie i jak szczegółowe były dyskusje na ten temat. To prawo już działa. Już mówimy o działającym prawie, które jest jednakowoż w okresach przejściowych. *Vacatio legis*

jest tak rozpisane, że minie jeszcze parę miesięcy, zanim wszystkie kluczowe podmioty będą miały wszystkie obowiązki. Więc to już zrobiliśmy m.in. staraniem tej Komisji.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Bardzo dziękuję.

Długie dyskusje były przede wszystkim spowodowane nadregulacją w stosunku do prawa unijnego. Tutaj była jedynie jakakolwiek uwaga środowisk. Myślę, że wszyscy na tej sali i w parlamencie popieraliśmy słuszość KSC.

Bardzo proszę, pan przewodniczący Napieralski.

**Posel Grzegorz Napieralski (KO):**

Bardzo dziękuję, panie przewodniczący.

Zacznę tak trochę filozoficznie, od takiego stwierdzenia, które pojawia się bardzo często w różnych debatach, ile jest bezpieczeństwa, ile wolności w naszym życiu. Jak się okazuje, im więcej wolności, tym więcej niebezpieczeństwa. Myślę, że to jest też chyba dyskusja na naszą Komisję.

Jeżeli dobrze zrozumiałem z tego, ale będę dopytywał pana ministra, to jest tak, że po prostu pojawił się na rynku podmiot, zdobył zaufanie innych w tym medycznych podmiotów i zbudował ofertę. Oferta, którą zbudował, została zaakceptowana, a później ktoś się włamał do tej firmy i po prostu te dane najprawdopodobniej wykradł, bo nie mamy pewności, co się wydarzyło.

Mam takie pytanie. Panie ministrze, szanowni państwo, jak pokazalibyście to tak na osi czasu? Rozumiem, że ta firma w jakimś momencie powstała, miała jakiś swój moment funkcjonowania na rynku. Skoro tyle podmiotów podpisało z nią porozumienie... Rozumiem, że większość tych podmiotów to były podmioty, które są finansowane przez Narodowy Fundusz Zdrowia, więc te kontrakty musiały być zawierane. Czy w tamtym czasie były jakiegolwiek przepisy prawa, które mogłyby dawać komuś możliwość ingerencji państwa, żeby, nie wiem, monitorować, prosić o raporty, prosić o informacje?

Mnie przeraziła jeszcze jedna informacja... Chodzi o rozmowę o prywatnych firmach, które mają dostęp do informacji o naszych dzieciach. Czy my w takim razie jesteśmy tu prawnie zabezpieczeni? Skoro ustawa została zawetowana przez pana prezydenta i dalej te dwie firmy... Czy nie ma zagrożenia? Czy możemy mieć jakąś wiedzę na temat tych firm i zbierania tych danych? Czy one w takim razie są dobrze zabezpieczone?

Pytam, żeby mieć wiedzę, czy jest bezpiecznie. Nie chcę kontrolować żadnych danych, żeby była jasność. Nie interesuje mnie, czy MyDr, czy jak on tam się nazywa, ma takie recepty czy inne. Chciałbym tylko wiedzieć, że recepty mojej mamy... Ja tam nie mam z tym problemu, mogę opowiedzieć o swoich receptach. Ale czy recepty mojej mamy, moich znajomych, ludzi, którzy siedzą na tej sali, są bezpieczne? Czy dane dzieci, szczególnie w tym trudnym czasie, kiedy tak naprawdę mamy problemy w sieci, są zabezpieczone?

Mam wrażenie, że przez te ileś lat, wiedząc dokładnie o wszystkich zagrożeniach, nie budowaliśmy systemu bezpieczeństwa. Tu chyba będę się jednak trochę różnił z panem przewodniczącym w podejściu do sprawy – uważam, że jednak czasami trzeba zrezygnować z odrobiny wolności na rzecz naszego bezpieczeństwa. Jeżeli nie będziemy mogli monitorować takich rzeczy... Rozumiem, że to jest prywatna firma. Też nie mam z tym żadnego problemu, panie przewodniczący. Tylko jeżeli ta prywatna firma ma dostęp do tak wrażliwych danych, które mówią o naszym zdrowiu, to musi podlegać jakimś specjalnym przepisom.

W wielu miejscach przyjęliśmy takie przepisy, że nawet prywatne firmy w wielu sytuacjach muszą odpowiadać odpowiednim normom, żeby funkcjonować. Są specjalnie przeświecane, sprawdzane i działają. Więc zastanawiam się, co się stało, że przez te lata... Bardzo przepraszam, nie sprawdziłem tego. Nie wiem, od kiedy oni tak naprawdę są na rynku tak aktywnie. Rozumiem, że są jakimś potentatem, skoro mają tyle tysięcy podpisanych umów. Co się stało, że nie mamy takich przepisów? Czy nikt nie kontrolował ich wtedy, nie kontrolował ich teraz?

Rozumiem, że jest propozycja pana premiera Gawkowskiego, z czego się bardzo cieszę. Ona w takim razie jest absolutnie na czasie. Nie wiem, czy pan dyrektor, czy pan minister – jest to dla mnie obojętne – jeżeli mogliby się o tym wypowiedzieć, trochę to nam przybliżyć...

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję. Momencik, panie przewodniczący, ale ja właśnie o tym mówiłem, tak? Istnieje firma prywatna i też mnie to dziwi, dlaczego do dnia dzisiejszego takie firmy nie są audytowane.

Chyba że są, ale nie usłyszeliśmy tego dzisiaj, że są audytowane. Audytowane przede wszystkim pod kątem bezpieczeństwa danych.

**Sekretarz stanu w MC Michał Gramatyka:**

Ja odpowiem.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Bardzo chętnie posłucham. O to właśnie chodzi. Tutaj się zgadzamy. Uważam, że podmioty prywatne również mogą działać na danych wrażliwych, tylko powinny być kontrolowane przez państwo. To bezpieczeństwo danych jest w interesie nas wszystkich. Bardzo proszę.

**Sekretarz stanu w MC Michał Gramatyka:**

Bardzo dziękuję.

Oczywiście, że istnieją takie regulacje. Te regulacje istnieją na wspólnym rynku w Europejskim Obszarze Gospodarczym. Ta regulacja nazywa się GDPR, czyli czy na General Data Protection Regulation. Po polsku to się nazywa ustawa o ochronie danych osobowych. Tam wszystko jest bardzo precyzyjnie opisane: jakie elementy należy zachować, jakie dane podlegają ochronie, jakie są kary, kto jest urzędem nadzorującym. W tym przypadku ten urząd nadzorujący też działa. To, co my identyfikujemy jako zadanie legislacyjne do zrobienia, to jest jak gdyby pochodna tej sytuacji.

Proszę zwrócić uwagę na to, że została zaatakowana nie firma, która jest administratorem tych danych osobowych, tylko firma, która jest upoważniona do ich przetwarzania. Na razie nie widzieliśmy w polskim prawie, że są takie firmy, które mogą koncentrować bardzo duże ilości danych, nie będąc ich administratorami, nie będąc zobowiązanymi ze względu na RODO. Oczywiście one też muszą realizować obowiązki wynikające z RODO. Natomiast w naszej ocenie, bo pewnie przedstawiciele tej firmy by się z nami nie zgodzili, niedostateczny poziom bezpieczeństwa spowodował, że ktoś te dane im ukradł.

Ta firma jest rzeczywiście w posiadaniu bardzo dużej firmy od 2023 r. Została dokonana akwizycja tej firmy przez Grupę DocPlanner, właściciela m.in. portalu Znany Lekarz. Trwają kontrole Urzędu Ochrony Danych Osobowych w tej firmie. Pewnie będą też podejmowane jakieś administracyjne postępowania wobec tej firmy. To rzeczywiście udało się nam zidentyfikować. Pędzimy z legislacją, żeby w każdym przypadku, kiedy dochodzi do tak dużej koncentracji danych, państwo po prostu miało możliwość działania. Na razie tego nie widzieliśmy. Można powiedzieć, że uczymy się na błędach. Tak, to rzeczywiście był błąd. Ale też nikt wcześniej na to nie wpadł, że taka sytuacja może się może się zdarzyć, prawda?

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję bardzo.

Pan przewodniczący Stefaniuk, bardzo proszę.

**Poseł Dariusz Stefaniuk (PiS):**

Bardzo dziękuję, panie przewodniczący.

Panie ministrze, to chyba nie jest jednak pierwszy raz, gdy to się zdarzyło. To był pierwszy raz na taką skalę, natomiast przecież wiemy, że wycieki danych miały miejsce.

Mam pytanie do pana ministra. Jest mowa o tym, że będą środki zaradcze, o które pytał pan przewodniczący Pejo. Ja już też słyszałem to w mediach, teraz pan minister też potwierdził, że będą audyty czy też nakaz audytów i sprawdzania firm, które mają ponad 100 tys. danych osób czy 100 tys. osób w swoich bazach, tak? To dobrze to zrozumiałem. Tak.

Ile jest w Polsce firm, które mają taką liczbę osób? Nie chodzi tylko o polskie firmy, tylko po prostu: Ile jest takich firm działających na polskim rynku? Dlaczego 100 tys., a nie 50, nie 75, nie 150 tys.? Skąd wzięliście to 100 tys.? To jest drugie pytanie.

Trzecie pytanie: Czy toczy się śledztwo prokuratury w sprawie wycieku tych danych? Rozumiem, że szukamy sprawców. Chyba jeszcze ich nie znaleziono? Mówię o tych 19 mln. Czy toczy się śledztwo? Pytam też w kontekście firmy MyDr. Czy oni spełnili wszystkie obowiązki? Czasami jest złodziej, który nam kradnie, a czasami jest to po prostu spowodowane błędem ludzkim: świadomym lub nieświadomym.

Czy projekt, o którym mówicie w mediach, jest już gotowy? Czy macie go napisanego? Kiedy będzie złożony do Sejmu? Kiedy zacznie się certyfikacja tych firm? Ile czasu jeszcze upłynie?

Będziemy go przygotowywać i przygotowywać, a może za miesiąc znowu nam ktoś to ukradnie. Czy to będzie za miesiąc, za dwa, za trzy? Chcielibyśmy wiedzieć.

Pan minister słusznie wspomniał – to też miało być jedno z moich pytań – o e-dzienniku, żebyśmy tylko nie myśleli o temacie zdrowia, bo tak lubimy wchodzić w takie szuflady, ale jest cała masa dzieci, cała masa studentów. Tych danych jest wszędzie bardzo dużo. Myślę, że na poziomie e-dziennika to jest na pewno powyżej 100 tys., bo te dwie firmy, jak pan minister wspomniał, to jest 90–95% rynku. Zresztą rozmawialiśmy o tym na połączonym posiedzeniu Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Komisji Edukacji i Nauki. Myślę, że temat jest pilny, my go trochę bagatelizujemy, że nic się nie stało. Dzięki Bogu, że nic się nie stało, chociaż dane kolegów wyciekły. Moje nie wyciekły. Na razie mogę się cieszyć. Sprawdzałem.

Natomiast myślę, że mogą to być kwestie... Skoro premier Donald Tusk mówi, że mamy zagrożenie i mamy wielką, wzmożoną aktywność Rosji na jesieni, w zimie – słyszeliśmy to od premiera, są to słowa kluczowe – to dlaczego ta aktywność nie może się przełożyć na przykład na kradzież tego typu danych, handel tymi danymi? Chodzi nie tylko o numery PESEL, ale megawrażliwe dane. Czy państwo sobie z tego zdajecie sprawę i czy projekt będzie w miarę jak najszybciej w Sejmie? Czy pan minister jest w stanie to powiedzieć? Bardzo dziękuję.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję.

Proszę, panie ministrze.

**Sekretarz stanu w MC Michał Gramatyka:**

Znowu zacznę od końca.

Nie, nikt nie bagatelizuje tej sytuacji. To, że ja mówię, że te dane nie zostały nigdzie wystawione, że nie udało się ich znaleźć w darknecie czy na forach przestępców, to jest generalnie szczęście w nieszczęściu. To jest najpoważniejszy wyciek czy najpoważniejsze przestępstwo, z którym mieliśmy do czynienia od lat. Podejmowane są wszelkie środki zaradcze. Pracuje zarówno Agencja Bezpieczeństwa Wewnętrznego, jak i CSIRT, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego w NASK. Prokuratura Okręgowa w Warszawie prowadzi śledztwo za pomocą cyberpolicji w tym zakresie. Jest prowadzona seria kontroli w firmie, która odpowiadała za przetwarzanie tych danych, tak że państwo podejmuje wszystkie przewidziane prawem możliwości, żeby po pierwsze uniknąć takiej sytuacji na przyszłość, a po drugie, by znaleźć osoby odpowiedzialne za to przestępstwo.

One zresztą dużo robią, żeby pozostać anonimowe. Szczęściem w nieszczęściu trafiło na tzw. białe kapelusze. Nie wiem, czy państwo wiedzą, ale wśród hakerów jest taki podział nawiązujący do tego, że w latach pięćdziesiątych w amerykańskich westernach dobre charaktery nosiły zawsze jasne kapelusze, a czarne charaktery nosiły czarne kapelusze. To się przeniosło do grup hakerskich, można się spotkać z takim sformułowaniem. Białe kapelusze to tacy hakerzy, którzy wykorzystują swoją wiedzę do testowania odporności systemów państwowych. Bardziej informują o tym, gdzie są dziury, żeby umożliwić ich załatanie. Nie są przestępcami, którzy wykradają dane po to, żeby żądać okupu albo żeby potem handlować tymi danymi, albo żeby tymi danymi kogoś szantażować. Myślę, że o efektach tego śledztwa będziemy informowani stosownym trybem.

Legislacja już jest. Ona idzie szybką ścieżką rządową. Chcemy zrobić tak, żeby maksymalnie ograniczyć proces konsultacji tej legislacji. Zwracam uwagę, że będzie to współpraca co najmniej trzech resortów: resortu zdrowia, resortu cyfryzacji i władz administracji odpowiedzialnej za ochronę danych osobowych. Wiem, że te prace już się toczą, że te przepisy powstają. Kiedy one będą w Sejmie? Trudno mi odpowiedzieć, ale jestem przekonany, że jeszcze w tym roku.

Dlaczego 100 tys.? Trzeba było przyjąć jakiś próg, który z jednej strony nie wpędzi w zwiększone obowiązki miasteczek, które mają rejestr swoich obywateli i wydają im kartę lojalnościową, na przykład karta mieszkańca miasta Tychy. Ona nazywa się u mnie AZetka. Nie wiem, jak nazywa się taka karta w Białej Podlaskiej.

**Poseł Dariusz Stefaniuk (PiS):**

Jest taka karta. A ile Tychy mają...

**Sekretarz stanu w MC Michał Gramatyka:**

130 tys. mieszkańców.

**Posel Dariusz Stefaniuk (PiS):**

Ale ile wydali kart? To o to chodzi.

**Sekretarz stanu w MC Michał Gramatyka:**

Myślę, że poniżej 100 tys. Generalnie chodzi o to, żeby to działało pozytywnie, żeby nie zabijało fajnych inicjatyw, więc przyjęto taki próg 100 tys. Czy on jest dobry, czy nie, to pewnie jeszcze nam wyjdzie na etapie konsultacji. Bardzo dziękuję.

**Posel Dariusz Stefaniuk (PiS):**

Tylko chciałem dopytać: Dlaczego konsultujecie to tylko z Ministerstwem Zdrowia? Znowu mówię, żebyście się nie zamykali w tych szufladach. Sam pan minister powiedział o e-dzienniku. Dlaczego też na przykład nie edukacja? Dlaczego nie nauka? Po co się tak zamykać tylko na zdrowie? Za chwilę zrobimy ustawę. Ona będzie tylko ukierunkowana, ale ten wyciek akurat MyDr... Tam może być każdy inny portal i okaże się, że mamy dziurę w zupełnie innym miejscu. Kibicuję, żeby to się udało, bo chodzi o to, żebyśmy się nie ośmieszali jako państwo, jako rząd, natomiast polecam to rozszerzyć.

**Sekretarz stanu w MC Michał Gramatyka:**

Jak pan przewodniczący zapewne wie, każdy projekt rządowy jest konsultowany przez wszystkie resorty. Mówię po prostu, że co najmniej trzy resorty są zainteresowane pracą nad tą legislacją, więc to pewnie przejdzie przez wszystkie resorty. Zresztą system certyfikacji jest już dość precyzyjnie określony, tyle że jest jeszcze nieobowiązkowy. Wprowadzimy obowiązki przy przekroczeniu progów. Tak że to jest słuszna uwaga. Bardzo dziękuję.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Chciałem dopytać, panie ministrze. Czy sprawcy tego wycieku zostali ujęci? Czy wiemy, kto to jest? Pytam o to bardziej na bazie pana wypowiedzi przed momentem, że to są białe kapelusze. Skąd wiemy, że to są białe kapelusze? Tylko dlatego, że jeszcze nie wykorzystali tych danych, a mogą je wykorzystać? Czy faktycznie wiemy, kto jest w posiadaniu tych danych?

**Sekretarz stanu w MC Michał Gramatyka:**

Nie mam dostępu do materiałów postępowania. Postępowanie jest prowadzone pod nadzorem Prokuratury Okręgowej w Warszawie przez cyberpolicję. Mówię państwu to, czego się dowiaduję z domeny publicznej. W domenie publicznej jest opisywana forma kontaktu z tymi włamywaczami, więc mówię to, co czytam. Obawiam się, że będzie trudno ich ująć. Te osoby robią dość dużo, żeby zachować anonimowość. Natomiast jakie będą wyniki śledztwa, to jest pytanie nie do mnie.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dobrze, dziękuję bardzo.

Pan poseł Łukaszewicz, proszę bardzo.

**Posel Sebastian Łukaszewicz (PiS):**

Dziękuję bardzo, panie przewodniczący.

Panie ministrze, trochę śmiesznie brzmi w pana ustach wybielanie tego, co się stało. Jeśli pan mówi, że ta grupa zapowiedziała, że nie zamierza korzystać z tych danych, nie zamierza ich sprzedawać, pan mówi o nich per białe kapelusze, bo testują różnego rodzaju systemy odporności państwa, a nagle wycieka 19 mln rekordów, to jest to trochę takie nieudolne tłumaczenie. Rozumiem próbę szukania ucieczki, ale wydaje mi się, że wyciek 19 mln rekordów jest zbyt poważnym, żeby mówić o tym, że jest to testowanie odporności państwa.

Szanowni państwo, kilka dni temu pojawiła się zapowiedź, oświadczenie tychże ludzi, którzy dokonali tego ataku. Jest to oświadczenie chyba sprzed pięciu dni, które mówi, że planują coś większego, że planują kolejny atak, o którym mamy się niedługo dowiedzieć.

W związku z tym mam pytanie. Czy Ministerstwo Cyfryzacji bądź Computer Emergency Response Team Polska (CERT Polska) słyszało o tym oświadczeniu? Czy wiedzą państwo, jakiego podmiotu może on dotyczyć? Czy śledzicie to, co dotyczące tych zapowiedzi dzieje się w domenie cyber? Żeby zaraz się nie okazało, że wyciekną nam dane z Krajowego Systemu e-Faktur i będziecie mówić, że to znowu było testowanie odporności państwa.

Mam pytanie: Czy po prostu śledzicie te komunikaty, które pojawiły się cztery czy pięć dni temu ze strony ludzi, którzy przypisują sobie atak na MyDr?

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Proszę bardzo, panie ministrze.

**Sekretarz stanu w MC Michał Gramatyka:**

Nie chcę się wdawać w jakieś beznadziejne dyskusje ani nie tłumaczę się. Ja po prostu mówię o tym dlatego, że w języku potocznym używa się sformułowania haker zwykle w kontekście negatywnym, podczas kiedy haker może mieć wymiar pozytywny. Haker to jest osoba, która dysponuje specjalistyczną wiedzą. Mój wtęt o białych i czarnych kapeluszach raczej był zorientowany na to, że nie wszyscy hakerzy są źli. Hakerzy pracują w NASK, w Agencji Bezpieczeństwa Wewnętrznego. Stoją na straży integralności i bezpieczeństwa systemów państwowych. To są tacy sami hakerzy, jeżeli chodzi o ich umiejętności, jak ci pracujący czy tam działający po tej ciemnej stronie.

Tak, znam te wpisy, o których pan mówi. To są wpisy z Fediverse, czyli ze społecznościowego odpowiednika X czy tam Twittera. Konkretnie chodzi o jeden wpis stanowiący korespondencję z bardzo profesjonalnym dziennikarzem portalu Zaufana Trzecia Strona. W tym wpisie rzeczywiście mówią, że „za chwilę pokażemy wam coś znacznie większego”, nazywają wszystkich innych dziennikarzy i polityków kłamcami. W tym wpisie pojawia się jeszcze parę innych epitetów.

Tak, oczywiście monitoring wszystkich systemów państwowych jest prowadzony na co dzień. Nie trzeba nam takich nieszczęśliwych wydarzeń, nie trzeba nam takich przestępstw, żebyśmy prowadzili monitoring integralności systemów państwowych. Codziennie dostajemy informacje, ile było prób ataków, ile było incydentów, ile zdiagnozowano takich incydentów, czy są jakieś alerty, które raportuje nam NASK. Cały system cyberbezpieczeństwa państwa jest podzielony pomiędzy trzy zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT-y), które ze sobą współpracują. Te CSIRT-y mają renomę nawet nie tylko europejską, ale światową. Uczestniczą w międzynarodowych spotkaniach takich właśnie służb, gdzie dzielą się swoim doświadczeniem.

Uważam, że jako państwo mamy wysoki poziom cyberbezpieczeństwa. Od początku powtarzam, że to nieszczęśliwe wydarzenie dotknęło firmę prywatną, a wszyscy rozmawiamy o tym właśnie dlatego, i rozmawiamy o tym bardzo poważnie, że ofiarą tego przestępstwa padły dane około 18 mln Polek i Polaków. Dlatego jest interwencja państwa i dlatego jest nasze spotkanie. Nikt tutaj, nie wiem, ani niczego nie obraca w śmieszność, ani nie unika odpowiedzialności – wręcz przeciwnie. Czuję pełną odpowiedzialność za to, żebyśmy wszyscy czuli się bezpiecznie w tym cyberświecie.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję bardzo.

Tak, jeszcze pan poseł.

**Poseł Sebastian Łukaszewicz (PiS):**

Czy próbowaliście nawiązać kontakt poprzez portal, o którym pan mówił, z ludźmi, którzy wrzucili to oświadczenie do sieci?

**Sekretarz stanu w MC Michał Gramatyka:**

Panie pośle, jeszcze raz mówię, że cytuje pan wpisy z Fediverse. Nie da się nawiązać do wpisu. Można wysyłać tweety albo można wysyłać wpisy na Mastodonie, ale czy to jest forma nawiązywania kontaktu? Przecież, jeżeli ja jako Ministerstwo Cyfryzacji wpiszę na Mastodonie, że nie jesteśmy politycznymi kłamcami, tylko odpowiedzialnymi ludźmi, to pan nie zostawi na mnie suchej nitki na tej Komisji. Więc jeżeli...

**Poseł Sebastian Łukaszewicz (PiS):**

Panie ministrze, jesteśmy inteligentnymi ludźmi, przecież doskonale pan wie, że można przeprowadzić taką operację w inny sposób, niekoniecznie pisząc do ludzi i podpisując się „Michał Gramatyka, wiceminister cyfryzacji”. Bądźmy poważni.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dobrze, szanowni państwo...

**Poseł Grzegorz Napieralski (KO):**

Panie pośle, jak chcemy poważni, to też są służby od tego, a nie pan minister Gramatyka czy my. Bardzo proszę, nie powinniśmy nawet prowadzić takiej dyskusji.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Pan poseł Bliźniuk, bardzo proszę.

**Poseł Paweł Bliźniuk (KO):**

Dziękuję, panie przewodniczący.

Wysoka Komisjo, panie ministrze, jeżeli chodzi o wdrażanie KSC, to rozmawialiśmy o tym na podkomisji do spraw cyberbezpieczeństwa jeszcze przed sierpniową przerwą. To jest proces i on oczywiście ma już... Jest w pewnym studium zaawansowania, ale trzeba też pamiętać, że realne dostosowanie systemu do obowiązującej litery prawa zajmuje czas. Zresztą mamy terminy przewidziane przez prawo.

Natomiast mam kilka uwag. Trzymajmy się jak najdalej od spekulacji, bazujmy na faktach. Dobrze, że pan minister nazywa to, co się wydarzyło, przestępstwem. Mamy osoby, które są sprawcami. Pewnie są poszukiwane przez odpowiednie, powołane do tego organy. Niech te organy zajmują się tym w reżimie, kto jest przewidziany przez prawo.

Nie mogę się zgodzić ze stwierdzeniem, że państwo polskie nie ma żadnych regulacji dotyczących kontroli podmiotów prywatnych, które przetwarzają albo dane wrażliwe, albo dane na dużą skalę. Tą regulacją jest oczywiście RODO i przepisy wdrażające regulacje unijne do naszego porządku prawnego. Tam są przepisy wprost mówiące o możliwości kontrolowania sposobu przetwarzania danych przez podmioty prywatne. Ta metoda i ten sposób – cała ta ścieżka jest opisana.

Pytanie z naszej strony – jak to wygląda, czy takie podmioty są kontrolowane w jakiś metodyczny sposób, czy jest jakiś plan kontroli – powinno być skierowane do Urzędu Ochrony Danych Osobowych. Oczywiście zgodnie z przepisami po stronie administratora jest też nie tylko jednorazowe wprowadzenie zabezpieczenia, a również weryfikacja tych zabezpieczeń, ocena ryzyka ze względu na sposób, rodzaj przetwarzanych danych, skalę przetwarzania danych itd. Mam nadzieję i jestem przekonany o tym, że to jest też przedmiotem badań ze strony prokuratury.

Oczywiście KSC ma wprowadzić obowiązek daleko idących wymagań co do ochrony tych danych, ale też de facto można powiedzieć, że one powinny być proporcjonalne już na bazie obowiązujących dzisiaj przepisów, przede wszystkim na bazie RODO, więc te przepisy są. Pytanie brzmi, jak one są wdrożone, jak wygląda ich stosowanie. Teraz ta dyskusja jest bardziej aksjologiczna i też być może szersza. Mamy kontekst danych wrażliwych, danych obywateli i obywateli. Pytanie, na które dzisiaj pewnie nie udzielimy sobie odpowiedzi, to jest pytanie o model, który powinniśmy wybrać, jeżeli chodzi o przetwarzanie tych danych. Czy powinniśmy utrzymywać model, w którym jest rynek i to podmioty prywatne w obowiązującym reżimie prawnym powinny przetwarzać te dane, czy też je gromadzić? Czy też gdy dane są tak wrażliwe, powinniśmy szukać rozwiązań na poziomie krajowym, gdzie administratorem jest państwo w różnych swoich formach?

Mieliśmy taką dyskusję, jak procedowaliśmy kwestie e-dziennika, czyli rozwiązania, które stanowiło propozycję, by to państwo przetwarzało dane uczniów. A chodzi o dane, które też mogą być i są na tyle wrażliwe, że mogą stanowić podstawę do profilowania osób na przyszłość, to nie tylko dane tu i teraz, jeżeli chodzi o jakieś informacje gromadzone w sposób przypadkowy. Wygrała – przynajmniej na poziomie Sejmu – opcja, że powinniśmy jednak centralizować i obarczyć państwo polskie odpowiedzialnością za przetwarzanie tych danych, ale też za jakość zabezpieczeń. Jak widać, jeżeli dochodzi do jakiegoś kryzysu czy też przełamania zabezpieczeń, może nieprawidłowego stosowania obowiązujących przepisów... Tego jeszcze nie wiemy, mam nadzieję, że będzie to sprawdzać prokuratura. Na końcu według obywateli, w takim ogólnym poczuciu odpowiedzialność za bezpieczeństwo danych wrażliwych (mówimy o danych medycznych) oraz za ochronę tych danych spoczywa na państwie polskim, instytucjach publicznych, a nie prywatnych. I słusznie.

Kolejną sprawą jest to, że rzeczywiście na podstawie obowiązujących przepisów po stronie administratora leży obowiązek poinformowania wszystkich, których dane wyciekły, o fakcie, że doszło do wycieku. Są przewidziane konkretne terminy w obowiązującym prawie, w RODO. Wszyscy powinniśmy zostać poinformowani o tym wycieku w sposób przewidziany przez przepisy, jeżeli doszło do wycieku. Mówię o administratorze, czyli znowuż w tym przypadku o podmiocie prywatnym.

To bardzo dobrze, że przez ministerstwo został wprowadzony mechanizm i możemy zweryfikować fakt, czy te dane wyciekły, czy nie. Natomiast trzeba pamiętać, że są przepisy, które nakładają taki obowiązek po stronie administratora. Jeżeli dochodzi do wycieku, to powinna być informacja do tych, których dane wyciekły, o skali wycieku, nie tylko samym fakcie. Więc trzeba

w tej dyskusji pamiętać o tym, wyciągnąć wnioski, bo jeżeli chodzi o rozliczenie tego konkretnego przypadku, to jest sprawa dla prokuratury i odpowiednich służb.

Z pewnym takim pozytywnym nastawieniem przyjmuję informację, że jest przygotowane rozwiązanie legislacyjne, które ma zaimplementować stosowne rozwiązanie do naszego porządku prawnego. Już też z tego miejsca na pewno sygnalizuję chęć zwołania podkomisji, w ramach której porozmawiamy na temat założeń tej ustawy. Chcemy, żeby ona jak najszybciej przeszła przez polski Sejm, chciałbym, żebyśmy się zaangażowali już na etapie nawet dyskusji i konsultacji na poziomie rządowym, żeby później nie było sytuacji, w której utkniemy z pracami legislacyjnymi na poziomie Sejmu. Myślę, że to jest dobry kierunek, żeby rozmawiać o tych rozwiązaniach, szczególnie pan wiceprzewodniczący, który teraz już wyszedł, ale też wskazywał, że być może trzeba rozmawiać o jakimś szerszym ujęciu tego zagadnienia, a nie ograniczać się tylko do ochrony zdrowia. Myślę, że to jest przedmiot, który powinniśmy podjąć w ramach prac samej podkomisji. Dziękuję.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję.

Panie ministrze, do tej wypowiedzi?

**Sekretarz stanu w MC Michał Gramatyka:**

Mnie pozostaje tylko podziękować za tę wypowiedź, w szczególności za sformułowanie tych wyzwań.

Zgadzam się z panem posłem, że to będzie aksjologiczna dyskusja, ale odbędziemy ją, dyskutując nad tą legislacją, bo ona prędzej czy później wpłynie na Komisję. Nie wyobrażam sobie, żeby Sejm ją przyjął bez opinii Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. Dziękuję bardzo.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję.

Czy ktoś z państwa chciałby zabrać głos? Bardzo proszę, pani Joanna i później pan.

**Członek Stowarzyszenia Absolwentów Elektroniki na Politechnice Warszawskiej @ELKAPW  
Joanna Karczewska:**

Dziękuję. Nazywam się Joanna Karczewska, jestem absolwentką Wydziału Elektroniki Politechniki Warszawskiej, zajmuję się cyberbezpieczeństwem, bezpieczeństwem informacji i ochroną danych osobowych.

Przygotowując się do dzisiejszego posiedzenia, sięgnęłam do raportów Najwyższej Izby Kontroli i okazuje się, że już w 2017 r. z kontroli o nazwie „Podlaski System Informacyjny e-Zdrowie” mogliśmy się dowiedzieć, że podmioty lecznicze nie dbają o pełne bezpieczeństwo danych wrażliwych. W 2019 r. była kolejna kontrola – na temat wdrożenia przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych. Znowu niemal w żadnym ze skontrolowanych podmiotów leczniczych dane osobowe pacjentów nie były prawidłowo chronione i przetwarzane.

Mamy rok 2023, kontrola pt. „Ochrona danych pacjentów przed cyberatakami w podmiotach leczniczych na terenie województwa warmińsko-mazurskiego”. Czytamy znowu: „Kontrolowane szpitale i przychodnie nie zawsze zapewniały prawidłową ochronę danych osobowych pacjentów przed cyberatakami”. Mamy najnowszą kontrolę, która dotyczyła zapewnienia ciągłości świadczenia usług medycznych w placówkach ochrony zdrowia na wypadek braku zasilania w energię elektryczną ze źródeł zewnętrznych i znowu: „brakuje rzetelnego serwisowania, aktualnych procedur i wymaganych instrukcji eksploatacyjnych”. Czyli mieliśmy już od dawna sygnały o tym, że się bardzo źle dzieje w ochronie zdrowia.

Sprawdziłam też, ile kar Urząd Ochrony Danych Osobowych nałożył od 2018 r., czyli od momentu obowiązywania RODO. Okazuje się, że razem było 10 kar nałożonych na różne podmioty lecznicze, ale tylko 5 dotyczyło bezpieczeństwa, czyli na podstawie kar nałożonych przez Urząd Ochrony Danych Osobowych wyglądało na to, że jest dobrze. Mieliśmy kontrolę NIK, że jest źle, a tutaj tylko 5 kar. Co więcej, 2 kary były milionowe. Reszta to były takie drobiazgi, bo to już były podmioty państwowe.

Sięgnęłam też do rejestru podmiotów wykonujących działalność leczniczą. Okazuje się, że na dzień wczorajszy aktywnych podmiotów leczniczych jest 281 087, a wyciek dotyczy tylko 12 tys. podmiotów leczniczych. Więc znowu: Czy jest dobrze, czy też źle, że chcemy raptem zmniejszać prawo? Razem dużych podmiotów leczniczych jest 29 tys., a później to już są drobiazgi typu

praktyki pielęgniarzek, praktyki lekarskie, praktyki fizjoterapeutyczne. Czy proponowana legislacja ma objąć tylko wybrane placówki medyczne, czy też spojrzeć szeroko na całe zagadnienie?

Pytanie zasadnicze i mówię to z kolei z praktyki: Kto ma egzekwować proponowaną piątkę dla zdrowia? Inspektorzy ochrony danych? Powiedziałabym, że z tym bardzo różnie bywa. Urząd Ochrony Danych Osobowych, jak widać, nałożył dotychczas tylko pięć kar za brak bezpieczeństwa. Wojewódzki sąd administracyjny, który bardzo intensywnie wypowiada się na temat testowania, mierzenia, oceniania skuteczności zabezpieczeń, a może pełnomocnicy do spraw cyberbezpieczeństwa?

Jesteśmy na początku drogi. Oczywiście jest Ministerstwo Cyfryzacji oraz NASK, równolegle Centrum e-Zdrowie, ale ile z tych ponad 300 tys. podmiotów leczniczych zagląda na strony czy to NASK, czy Centrum e-Zdrowie? Ostatnio nawet włączył się rzecznik praw pacjenta. Grzmiał, że trzeba przecież dbać o ochronę danych osobowych, bo to jest prawo pacjenta. Tyle że ten sam rzecznik praw pacjenta przyznał wyróżnienie wymagań jakości w maju tego roku centrum medycznemu, które 13 marca zostało objęte atakiem ransomware. Albo wymagamy jakości i uwzględniamy, że nie zadbali o bezpieczeństwo, albo sobie to odpuszczamy. W samym roku 2026 było ich już 9, i to poważnych. I to jest to, co pojawiło się w domenie publicznej.

Dziękuję za portal CyberDefence24.pl, który bardzo skrupulatnie relacjonuje różne przypadki cyberataków na placówki ochrony zdrowia.

Dlaczego podchodzę do proponowanych zmian legislacyjnych z pewnym sceptycyzmem? Otóż ja jestem po cyfrowej likwidacji przedszkola. Temat był poruszany w kontekście tego, że robimy coś dla zdrowia, a może też trzeba z myśłą o oświacie. Jestem po nieprawdopodobnie ciężkiej operacji zapewnienia cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych w trakcie likwidacji. To był koszmar. To było coś, czego nie życzę nikomu. Całe szczęście, że stałam za panią dyrektor i jej pomagałam. Przy samej likwidacji mogłoby dojść do wielu naruszeń ochrony danych osobowych i cyberbezpieczeństwa.

Proszę sobie wyobrazić, że musieliśmy zamknąć konta w systemach. Okazało się, że ich było 40. Przedszkole było nieduże, było 40 kont do zamknięcia z różnym skutkiem. Najtrudniej było z Ministerstwem Cyfryzacji przy systemie doręczeń. Najpierw trwa dyskusja, kiedy i jak zamknąć, a ostatecznie zamknęli nam konto ostatniego dnia rano, kiedy jeszcze czekaliśmy na pisma z Ministerstwa Edukacji Narodowej, kuratorium i ewentualnych dostawców systemów, że faktycznie nasze dane zostały usunięte z systemów. To było przywrócenie stanu fabrycznego sprzętu, utylizacja starego sprzętu, wypowiedzenie umów powierzenia przetwarzania. Jeden podmiot powiedział, że nie usunie powierzonych danych, że on jeszcze przez pół roku będzie je przetwarzać – uwaga – ze względów bezpieczeństwa. To było też wypowiedzenie różnych umów na usługi telekomunikacyjne i inne oraz archiwizacja, która okazała się tak trudnym zadaniem, że musiałam interweniować w Ministerstwie Edukacji Narodowej. Placówki lecznicze też są nieduże i też nie mają dużych funduszy na cyberbezpieczeństwo i ochronę danych osobowych, więc analogicznie, po moim doświadczeniu z przedszkolem, jestem sobie w stanie wyobrazić, jak to wygląda.

Przy okazji jako certyfikowany audytor systemów informatycznych swego czasu chciałam zaudytować e-dziennik, który obowiązywał już w tej chwili w przedszkolu. Nawet pisałam o tym publicznie. Otóż koszt tego to byłoby 30 tys. zł. Żadnego przedszkola nie stać na wyłożenie 30 tys. na audyt systemu e-dziennik. Więc jest opcja, jest możliwość, umowa powierzenia przetwarzania to przewiduje, natomiast dostawca życzył sobie wtedy za każdy dzień pracy przy audytorze 2 tys. zł. To był ich oficjalny cennik. Pisałam o tym w 2023 r.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Pani Joanno, przepraszam. Prosiłbym o puentowanie. Mamy ograniczony czas.

**Członek Stowarzyszenia @ELKApw Joanna Karczewska:**

Czy zostaną w ogóle wyciągnięte wnioski z sytuacji, która zaistniała, i z podobnej sytuacji przy okazji likwidacji przedszkola? Chodzi o cofnięcie się czy też uwzględnienie innych obszarów, w tym w szczególności oświaty. Dziękuję.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję bardzo.

Panie ministrze, proszę o ustosunkowanie się.

**Sekretarz stanu w MC Michał Gramatyka:**

Tak, zanim ta legislacja trafi do Sejmu, będziemy ją jeszcze opiniować na etapie rządu, na etapie komitetów rządu, więc myślę, że będziemy mieli nieraz okazję do tego, żeby dyskutować o tym prawie, o tym, jakich obszarów ono powinno dotyczyć i w oparciu o jakie reguły być podejmowane. To jest odpowiedź ad hoc. Nie jestem w stanie udzielić teraz głębszej odpowiedzi, dlatego że musiałbym przed sobą mieć tekst tej legislacji, a sam jestem na początkowym etapie jej przygotowywania. Bardzo dziękuję.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Bardzo dziękuję.

Jeszcze pan prosił o głos, proszę.

**Członek Rady Legislacyjnej Związku Pracodawców Polska Chmura Albert Szczepaniak:**

Dzień dobry. Albert Szczepaniak, Polska Chmura. Powiem tak zupełnie szczerze, że nie do końca przekonuje mnie argumentacja dotycząca tego, że ustawa o krajowym systemie cyberbezpieczeństwa jest w okresie przejściowym, jak również ta, która mówi o tym, że planowane są zmiany legislacyjne.

Pozwolę sobie zacytować państwu jedną rzecz. „Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, krajowy schemat specyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT i procesów ICT”. To jest art. 15 z ustawy o certyfikacji cyberbezpieczeństwa. Ta ustawa jest z nami od roku i od roku prosimy Ministerstwo Cyfryzacji jako związek o to, żebyśmy przystąpili jako kraj do przygotowywania takich schematów. Jesteśmy teraz w takim dosyć specyficznym punkcie, dlatego że zostaliśmy zaatakowani przez ludzi w białych kapeluszach, jak pan minister powiedział – tylko co w sytuacji, gdyby to nie były białe kapelusze? Co w sytuacji, w której hakerzy by nie poinformowali o tym, jaki jest wektor ataku? Co w sytuacji, w której musielibyśmy jako kraj ustalić, co się stało? Czy jako państwo mamy w ogóle możliwość przeprowadzania audytów wśród podmiotów, które znajdują się poza terenem naszego kraju? To jest jakby główne pytanie.

Tak się zastanawiam, bo pan minister powiedział, że poczuwa się do odpowiedzialności wobec tych rzeczy, które teraz będą wykonywane, do tej piątki zmian ustawodawczych itd. Czy pan minister poczuwa się do tego, że przez ostatni rok ten krajowy certyfikat nie został uchwalony, a może uratowałby dane 19 mln Polaków?

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję bardzo.

Ja też dodam takie pytanie. Pan zapytał o to, czy możemy audytować firmę spoza naszego kraju. Ja nadal nie widzę tej odpowiedzi: Czy my w tym momencie możemy audytować firmy w naszym kraju? To znaczy powiem inaczej – ta odpowiedź jest nadal niewypowiedziana, ale możemy się domyślać, że nie możemy albo nic się z tym nie dzieje.

Proszę.

**Członek Rady Legislacyjnej Związku Pracodawców Polska Chmura Albert Szczepaniak:**

Pozwolę sobie jeszcze dodać, że gdyby krajowa certyfikacja istniała i gdyby minister cyfryzacji przyjął rozporządzenie, zgodnie z którym zostałby ustalony schemat certyfikatu krajowego, to zgodnie z ustawodawstwem, który mamy już uchwalone, przyjęte i obowiązujące w tym kraju, jesteśmy w stanie audytować podmioty, które znajdują się na terenie Rzeczypospolitej Polskiej.

Problem jest inny. Zarówno MyDr, jak i podmiot, który agregował te dane – mówimy o centrach danych – to są podmioty zagraniczne i nie mamy żadnej siły przebicia. Zakładam, że Polska prokuratura nie jest w stanie pojechać teraz do Frankfurtu czy do Irlandii, żeby przeanalizować, czy wektor ataku przypadkiem nie przebiegał przez centra danych. Nie jesteśmy w stanie tego zrobić. Nie jesteśmy w stanie też zaudytować MyDr, a co więcej – MyDr właścicielsko jest spółką czy funduszem hiszpańskim. Więc na dobrą sprawę, gdyby oni nie chcieli z nami podjąć jakiegokolwiek współpracy, zakładam, że nie jesteśmy w stanie jako kraj wyciągnąć żadnego narzędzia, które pozwoliłoby nam ustalić, co się stało.

Chciałbym tylko uzyskać odpowiedź na jedno pytanie. Dlaczego w ciągu ostatniego roku ministerstwo nie podjęło żadnych działań, pomimo tego, że prosiliśmy o podjęcie takich działań, żeby krajowy system certyfikacji w końcu ruszył? Dziękuję.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję bardzo.

Proszę, panie ministrze.

**Sekretarz stanu w MC Michał Gramatyka:**

To rozporządzenie jest na etapie przygotowania. Gdyby to rozporządzenie było wydane, to i pan, i ja wiemy, że to nie jest obowiązkowa certyfikacja. To jest certyfikacja przeprowadzona na wniosek tych, którzy są wobec niej chętni, tych, którzy są nią zainteresowani.

Do kradzieży danych doszło na szkodę prywatnej firmy. Zostały skradzione dane z prywatnej firmy. Takie sytuacje się zdarzają. Legislacja, nad którą pracujemy, będzie zmierzała do tego, żeby taka certyfikacja była obowiązkowa również wobec prywatnych firm i żeby te prywatne firmy miały obowiązek podniesienia poziomu bezpieczeństwa tych danych. To, o czym pan mówi, o przechowywaniu danych, gdzie one fizycznie są zgromadzone – w kontekście danych państwowych ten temat jest rozwiązany. Wiemy dokładnie, gdzie są nasze dane. Mamy zastrzeżenia, że one muszą być w Europejskim Obszarze Gospodarczym i w jeszcze paru innych miejscach, najczęściej nawet na terenie Polski. Nie chcę tu w to wchodzić, dlatego że to przestępstwo dotyczyło prywatnej firmy.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję.

Proszę bardzo.

**Członek Rady Legislacyjnej Związku Pracodawców Polska Chmura Albert Szczepaniak:**

Jeszcze pozwolę sobie uzupełnić, dlatego że w m.in. naszych stanowiskach kierowanych do Ministerstwa Cyfryzacji podajemy przykład francuski.

Francja była stanie przyjąć ustawodawstwo, zgodnie z którym zobowiązała wszystkie podmioty na rynku prywatnym, które podejmują się działalności związanej z przetwarzaniem danych obywateli, w tym danych medycznych, żeby to były podmioty o strukturze właścicielskiej francuskiej, żeby centra danych, które agregują te dane, znajdowały się na terenie Francji. Udało się im to zrobić pomimo tego, że jesteśmy w Unii Europejskiej, pomimo swobody przepływu usług Unii Europejskiej. I to działa. Więc proszę mi wybaczyć, stąd też absolutnie nie jestem w stanie przyjąć argumentacji, którą przedstawia pan minister.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję.

Poruszył pan wątek naszej suwerenności technologicznej, bardziej cyfrowej. To może nie jest temat do końca na dzisiaj do rozwijania, ale oczywiście tak jest. Francja sobie potrafiła z tym poradzić, a my cały czas tkwimy w takim, można powiedzieć, zawieszeniu.

Panie ministrze, bardzo proszę. Czy mógłby pan się odnieść jeszcze do tych słów?

**Sekretarz stanu w MC Michał Gramatyka:**

To jest filozoficzna dyskusja. Możemy rozmawiać filozoficznie na temat tego, gdzie powinny być przechowywane dane w Polsce. Zaraz się narażę na zarzuty Konfederacji, że zmuszam prywatny biznes do tego, żeby funkcjonował w jednym obszarze geograficznym, prawda? Dlatego że jednak piewcy wolności na pewno nie pozostaną bezczynni. Mam swoje przekonania do tego tylko, że...

Ja też podchodzę z szacunkiem do wypowiedzi swojego przedmówcy, tyle że ta wypowiedź i ta dyskusja niestety nijak się mają do tego ataku. Nawet gdyby takie rozporządzenie było wydane, to te certyfikacje są dobrowolne. Nie ma obowiązku takiej certyfikacji. Szukamy w tym momencie rozwiązań legislacyjnych, które zabezpieczą nas na przyszłość. Jesteśmy na dobrej drodze, żeby takie legislacje się pojawiły.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Dziękuję bardzo.

Jeszcze pan, tak? To proszę. Ostatni raz, dobrze?

**Członek Rady Legislacyjnej Związku Pracodawców Polska Chmura Albert Szczepaniak:**

Tak, przepraszam, ale muszę. Tak, certyfikacje są dowolne, natomiast jesteśmy w stanie przyjąć jako kraj, że dana usługa musi podlegać danej certyfikacji. W związku z tym podmiot taki jak MyDr miałby dowolność w tym, czy jest certyfikowany, czy nie, ale jeśli chciałby świadczyć usługę,

która wymagałaby certyfikacji, to musiałby podlegać takiej certyfikacji. Niestety nie do końca jest tak, jak mi się wydaje, że pan minister rozumie.

**Sekretarz stanu w MC Michał Gramatyka:**

Czy ja też mogę się odnieść?

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Proszę się odnieść, oczywiście.

**Sekretarz stanu w MC Michał Gramatyka:**

To jest właśnie dokładnie drugi punkt z tej cyber piątki zaprezentowanej przez pana premiera Gawkowskiego. Dokładnie. Nawet sam lepiej nie byłbym w stanie go streścić, niż pan to przed chwilą zrobił.

**Członek Rady Legislacyjnej Związku Pracodawców Polska Chmura Albert Szczepaniak:**

Tylko że to już jest.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

We Francji już jest?

**Członek Rady Legislacyjnej Związku Pracodawców Polska Chmura Albert Szczepaniak:**

W Polsce.

**Przewodniczący poseł Bartłomiej Pejo (Konfederacja):**

Nie, jak w Polsce? Nie do końca.

Dobrze. Szanowni państwo, kończymy ten wątek. Ktoś z państwa jeszcze w tym temacie chciałby zabrać głos? Nie widzę.

Rozstańmy się taką z nadzieją, że będziemy w przyszłości reagować nie na konkretne incydenty, tylko wdrażać takie rozwiązania, żeby do takich incydentów nie dochodziło. Mam nadzieję, że kiedyś takie zasady nastaną.

Szanowni państwo, bardzo serdecznie dziękuję.

Zamykam dyskusję i zamykam posiedzenie Komisji.