Pojęcia kluczowe: *cyberbezpieczeństwo, tajemnica zawodowa, dobre praktyki*

Przemysław A. Barchan, Piotr Warchoł[1]

Dobre praktyki dotyczące cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata[2] – wprowadzenie

Abstrakt

Postępująca transformacja cyfrowa branży prawnej jest zjawiskiem nieodwracalnym, warunkującym działalność kancelarii prawnych niezależnie od ich wielkości. Proces ten niesie za sobą również wiele zagrożeń związanych z bezpieczeństwem infrastruktury informatycznej oraz bezpieczeństwem i poufnością danych znajdujących się w posiadaniu adwokata. W świecie cyfrowym przed ochroną tajemnicy adwokackiej stoi szereg wyzwań nie tylko natury prawnej, ale również technicznej i organizacyjnej.

Niniejszy artykuł stanowi zwięzłe przedstawienie *Dobrych praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata* (dalej: *Dobre praktyki*), które są jedną z odpowiedzi Naczelnej Rady Adwokackiej na wzrastającą liczbę cyberzagrożeń oraz potrzebę podnoszenia świadomości środowiska adwokackiego w zakresie cyberhigieny.

I. Cyberzagrożenia

Średnia tygodniowa liczba cyberataków na świecie w połowie 2023 r. na przeciętną organizację wyniosła 1258 razy (przy 1129 razach w Polsce). Utrzymuje się przy tym ogólnoświatowa tendencja corocznego wzrostu liczby ataków. Polska znalazła się jednak w 2022 r. w niebezpiecznym położeniu z uwagi na konflikt zbrojny na Ukrainie i działające wschodnie grupy hackerskie. Od października 2022 r. odnotowuje się wzrost średniej liczby ataków na polskie podmioty (przy czym w niektórych

1 Autorzy są adwokatami (Izba Adwokacka w Warszawie), współtwórcami Dobrych praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata wraz z adw. Pauliną Rzeszut (Izba Adwokacka w Katowicach) oraz adw. Adamem Baworowskim (Izba Adwokacka w Warszawie).

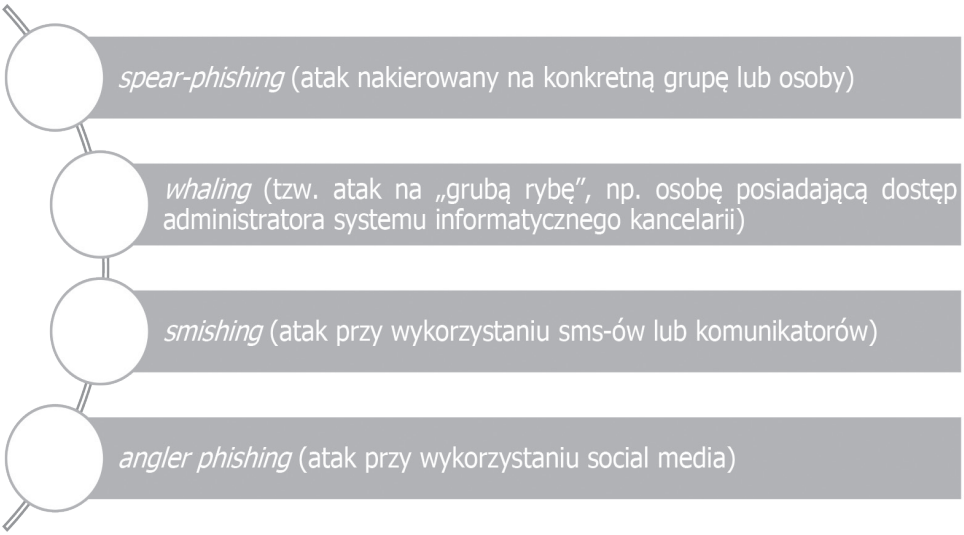
2 Aktualna treść dokumentu dostępna jest pod adresem: https://www.adwokatura.pl/z-zycia-nra/dobre-praktyki-cyberbezpieczenstwa-w-pracy-adwokata-i-kancelarii/ (dostęp: 21.01.2024 r.).

DOI: 10.54383/0031-0344.2024.01.9

sektorach gospodarki średnia liczba przewyższa 2500 razy tygodniowo). Średnia liczba cyberataków na świecie na przeciętny podmiot z branży prawnej przekracza 1000 razy tygodniowo[3].

Nie pozostaje to bez wpływu na bezpieczeństwo branży prawnej i przetwarzanych przez kancelarie danych, w tym danych objętych tajemnicą zawodową. Według opublikowanego 30.03.2023 r. przez wydawnictwo C.H. Beck raportu LegalTech 2023[4] 33% ankietowanych kancelarii miało styczność z cyberatakiem. Sygnalizujemy jednak, że w naszej ocenie dane te są znacząco zaniżone.

Dominującą formą ataków jest *phishing*[5], wykorzystujący działania socjotechniczne nakierowane głównie na wyłudzenie dostępów (np. haseł) lub kradzież środków finansowych. Podstawowymi środkami ataku *phishingowego* są korespondencja e-mail, komunikatory oraz *social media*, za pośrednictwem których ofiara otrzymuje link (najczęściej w formie podszywającej się pod znanego jej nadawcę)[6]. Główne formy *phishingu* to:



3 M. Duszczyk, *Polska jednym z kluczowych celów cyberprzestępców. Ataki rosną lawinowo*, „Rzeczpospolita", 5.01.2023 r., https://www.rp.pl/biznes/art37728661-cyberataki-polska-liczba-cele (dostęp: 4.09.2023 r.), https://crn.pl/aktualnosci/hakerzy-coraz-czesciej-atakuja-w-polsce/ (dostęp: 4.09.2023 r.).

4 Raport dostępny jest pod adresem https://legalis.pl/legaltech-raport-2023/

5 Inne to m.in. *ransomware* (atak mający na celu infrastrukturę i dane ofiary w połączeniu z okupem za przywrócenie dostępu do nich), *malware* (złośliwe oprogramowanie służące różnym celom, np. do przejęcia kontroli nad sprzętem), ataki DoS i DDoS.

6 Por. treść raportu The ENISA Threat Landscape (ETL) report, listopad 2022, dostępny pod adresem: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (dostęp: 25.02.2023 r.).

 DOI: 10.54383/0031-0344.2024.01.9

Dla zobrazowania potencjalnego ryzyka związanego z przetwarzanymi przez kancelarię danymi wskazujemy, że w posiadaniu kancelarii mogą znajdować się różne kategorie danych (m.in. dane stanowiące tajemnicę przedsiębiorstwa kancelarii, dane osobowe, dane objęte tajemnicą zawodową, inne dane prawnie chronione). Personel kancelarii przetwarza te dane w wielu środowiskach (m.in. w usługach on-line, w tym usługach chmurowych dostawców) i na różnorodnym sprzęcie (m.in. laptopy, tablety, smartfony, sprzęt drukujący).

W wielu sektorach gospodarki podmioty stosują dedykowane im lub powszechnie przyjęte standardy w zakresie bezpieczeństwa infrastruktury teleinformatycznej i informacji. Potrzebę wprowadzenia sektorowych wymogów w zakresie cyberbezpieczeństwa dostrzegł również ustawodawca unijny (m.in. dyrektywa NIS[7], dyrektywa NIS2[8], rozporządzenie DORA[9]). Kancelarie są gorzej zabezpieczone przed cyberatakami niż wielu klientów kancelarii. W przyszłości należy się zatem spodziewać znacznego wzrostu cyberataków na kancelarie. Z perspektywy atakującego skuteczniejsze może być podjęcie próby uzyskania dostępu do danych klienta kancelarii poprzez atak *phishingowy* skierowany na personel kancelarii niż podejmowanie próby bezpośredniego ataku na infrastrukturę klienta kancelarii.

Ze względu na powyższe zagrożenia zasadne stało się opracowanie podstawowych standardów cyberbezpieczeństwa dla kancelarii adwokackich[10].

II. Przebieg prac nad *Dobrymi praktykami*

Dobre praktyki zostały opracowane przez zespół ds. dobrych praktyk dotyczących cyberbezpieczeństwa Instytutu LegalTech przy Naczelnej Radzie Adwokackiej. Prace trwały 11 miesięcy, w okresie styczeń–listopad 2022 r. Prócz intensywnych prac wewnętrznych zespół konsultował treść *Dobrych praktyk* z zewnętrznymi partnerami (m.in. ze specjalistami z Politechniki Warszawskiej), a także z członkami samorządu adwokackiego (w ramach konsultacji środowiskowych przeprowadzonych w dniach 19.09.2022 r.–31.10.2022 r.). *Dobre praktyki* zostały ostatecznie przyjęte przez Naczelną Radę Adwokacką 14.01.2023 r.

7 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.07.2016 r., s. 1–30).

8 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022 r., s. 80–152).

9 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022 r., s. 1–79).

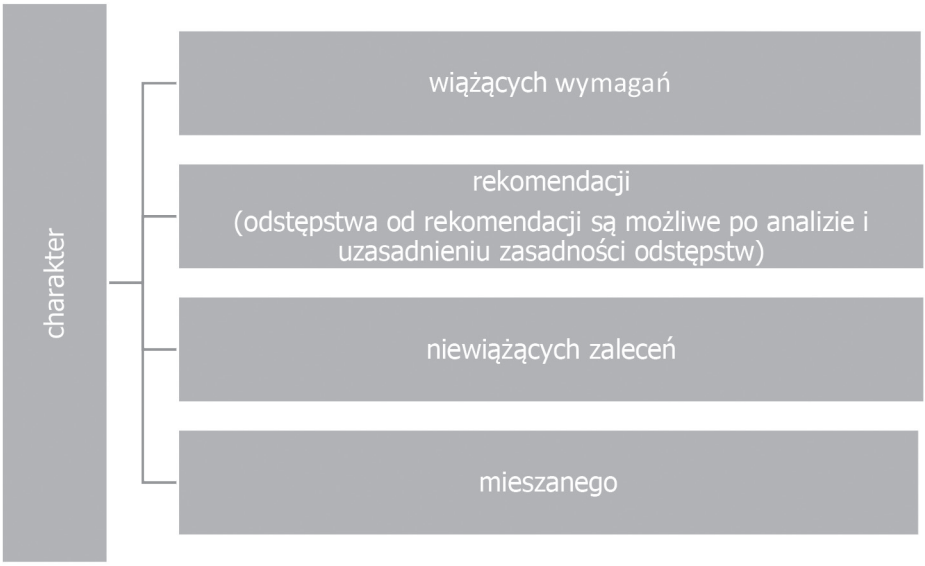
10 Jednym z pierwszych dokumentów w tym zakresie są wytyczne Cybersecurity Guidelines opracowane w 2018 r. przez International Bar Association's Presidential Task Force on Cybersecurity. Wytyczne dostępne są pod adresem: https://www.ibanet.org/MediaHandler?id=2F9FA5D6-6E9D-413C-AF80-681BAFD300B0 (dostęp: 25.02.2023 r.).

DOI: 10.54383/0031-0344.2024.01.9

III. Podstawa prawna i charakter *Dobrych praktyk*

Dobre praktyki stanowią załącznik do uchwały Naczelnej Rady Adwokackiej nr 86/2023 z 14.01.2023 r. W związku z tematyką objętą *Dobrymi praktykami*, tj. zaleceniami z zakresu cyberbezpieczeństwa, które są istotne z perspektywy zachowania tajemnicy zawodowej oraz zasad wykonywania zawodu adwokata, podstawy przyjęcia przez Naczelną Radę Adwokacką należy upatrywać w art. 3 ust. 1 pkt 5 oraz art. 58 pkt 12 ustawy z 26.05.1982 r. – Prawo o adwokaturze[11] oraz § 5 ust. 7 nowego Regulaminu wykonywania zawodu adwokata[12].

W trakcie prac nad *Dobrymi praktykami* autorzy rozważali kilka wariantów w zakresie charakteru prawnego *Dobrych praktyk*, tj. nadanie im charakteru:



Mając jednak na uwadze poziom trudności omawianego zagadnienia, a także konieczność podniesienia poziomu środowiskowej świadomości w zakresie cyberhigieny, przyjęto niewiążący charakter zaleceń ujętych w *Dobrych praktykach*. Oznacza to, że *Dobre praktyki* mają charakter zaleceń, których stosowanie nie jest obligatoryjne, a brak ich stosowania nie rodzi bezpośrednich negatywnych skutków w odpowiedzialności zawodowej czy dyscyplinarnej. Nie wyłącza to jednak obowiązków adresatów *Dobrych Praktyk* w zakresie dołożenia należytej staranności w dochowaniu tajemnicy zawodowej, określonych przepisami prawa i aktów samorządu adwokackiego, w szczególności regulujących zasady etyki zawodowej adwokata.

11 Dz.U. z 2022 r. poz. 1184, dalej: Prawo o adwokaturze.

12 Uchwała nr 140/2023 z 1.12.2023 r. – Regulamin wykonywania zawodu adwokata, obowiązująca od 1.01.2024 r., dalej: Regulamin

DOI: 10.54383/0031-0344.2024.01.9

IV. Adresaci *Dobrych praktyk*

Zalecenia ujęte w *Dobrych praktykach* adresowane są do różnych grup adresatów. Są to: (i) kancelarie, (ii) adwokaci, (iii) aplikanci adwokaccy, (iv) adwokaci i aplikanci adwokaccy świadczący swoje usługi jako prawnik i*n-house,* a także (v) prawnicy zagraniczni[13].

Zdecydowana większość kancelarii adwokackich w Polsce[14] prowadzona jest w składzie 1–3-osobowym. Mając to na uwadze, a także ewentualne różnice w zabezpieczeniach mogące wynikać z działalności zespołowej, *Dobre praktyki* rozróżniają kancelarie na: (i) jednoosobowe, (ii) małe (2–10-osobowe), (iii) średnie (11–20-osobowe) oraz (iv) duże (powyżej 20 osób). Kancelarie jednoosobowe tworzą adwokaci prowadzący kancelarie w formie jednoosobowych działalności gospodarczych, którzy swoją praktykę prowadzą samodzielnie, tj. bez zatrudniania stałego personelu kancelarii.

W celu prawidłowego ustalenia stanu liczbowego personelu kancelarii (prawnicy oraz personel pomocniczy) należy uwzględnić wspólników kancelarii, pracowników oraz stałych współpracowników kancelarii. Przez stałych współpracowników kancelarii należy rozumieć osoby, z którymi kancelaria zawarła umowę cywilnoprawną (np. umowę o współpracę), a z umowy i praktyki wynika, że osoby te pełnią rolę stałych współpracowników kancelarii. Osoby współpracujące z kancelarią jako niezależny zewnętrzny współpracownik (np. *of Counsel*) powinny być traktowane jako osoba trzecia, z którą należy zawrzeć odpowiednie umowy lub której należy udzielić stosownych upoważnień.

Adwokaci i aplikanci adwokaccy współpracujący z podmiotami gospodarczymi lub instytucjami w charakterze prawnika *in-house* powinni podjąć starania uwzględnienia zaleceń objętych *Dobrymi praktykami* w zakresie, w jakim korzystają oni ze sprzętu lub infrastruktury informatycznej takiego podmiotu gospodarczego lub instytucji, w ramach możliwości technicznych i organizacyjnych udostępnionych przez ww. podmiot lub instytucję. Podstawowym zaleceniem w tym przedmiocie jest poinformowanie tych podmiotów lub instytucji o istnieniu *Dobrych praktyk*.

Dobre praktyki mają zastosowanie również do kancelarii prowadzonych w formie spółek osobowych, w których wspólnikami są również inne niż adwokaci osoby wykonujące zawody określone w art. 4a ust. 1 ustawy z 26.05.1982 r. – Prawo o adwokaturze[15].

13 Prawnicy zagraniczni wpisani na listę prawników zagranicznych przez właściwą okręgową radę adwokacką na zasadach określonych w ustawie z 5.07.2002 r. o świadczeniu przez prawników zagranicznych pomocy prawnej w Rzeczypospolitej Polskiej (Dz.U. z 2020 r. poz. 823 ze zm.).

14 Przewiduje się, że blisko 70%.

15 Dz.U. z 2022 r. poz. 1184 ze zm.

DOI: 10.54383/0031-0344.2024.01.9

V. Konstrukcja *Dobrych praktyk*

W celu prawidłowej interpretacji *Dobrych praktyk* należy zwrócić uwagę na konstrukcję dokumentu *Dobrych praktyk*. Składa się z: (i) wprowadzenia, (ii) definicji, (iii) części głównej, oraz (iv) załącznika. Każdy z ww. elementów *Dobrych praktyk* jest potrzebny do poprawnego ich zrozumienia. W szczególności należy zwrócić uwagę na zdefiniowane pojęcia, które stosowane są w całym dokumencie.

Część główna *Dobrych praktyk* dzieli się na dwa rozdziały. Rozdział I zawiera zalecenia podstawowe adresowane do wszystkich odbiorców. Z kolei rozdział II obejmuje zalecenia dodatkowe adresowane do kancelarii małych, średnich i dużych. Zalecenia zostały przy tym pogrupowane według podziału narzędziowego, organizacyjnego lub usługowego, co ma ułatwić odbiór zaleceń. Dzielą się one na kategorie: zalecenia ogólne (np. korzystanie z aktualnego oprogramowania), komputery PC i przenośne (np. stosowanie silnych haseł dostępowych), smartfon (np. wykonywanie kopii zapasowych), serwery i urządzenia NAS[16] (np. zapewnienie redundancji łączy i narzędzi sieciowych), komunikacja w sieci Internet (np. szyfrowanie komunikacji), poczta elektroniczna (np. szyfrowanie i hasłowanie załączników wiadomości e-mail), back-up (np. szyfrowanie kopii zapasowych), przetwarzanie danych w usługach online (np. stosowanie uwierzytelniania wieloskładnikowego), przekazywanie danych poza kancelarię (np. szyfrowanie danych), biura serwisowane (np. brak korzystania z ogólnodostępnej sieci wi-fi), komunikatory (np. szyfrowanie danych), obsługa zewnętrzna IT (np. nadzór nad zdalnym dostępem i realizowanymi czynnościami).

Z kolei załącznik do *Dobrych praktyk* zawiera opis i rozwinięcie zaleceń z części głównej *Dobrych praktyk*, pogrupowanych według zaleceń. Załącznik dzieli się również na dwa rozdziały (odpowiednio jak część główna). W naszej ocenie kolumna „WYJAŚNIENIA" powinna stanowić podstawową lekturę adresatów *Dobrych praktyk*.

VI. Zalecenia ujęte w *Dobrych praktykach* – rys ogólny

Zapoznając się z poszczególnymi zaleceniami *Dobrych praktyk*, warto zwrócić uwagę na źródła ich pochodzenia. Źródłem tym będą przepisy prawa i norm aktów samorządu adwokackiego, a także praktyka i doświadczenie w zakresie cyberbezpieczeństwa. Poszczególne zalecenia nie są również całkowicie nowym materiałem, który nie został dotychczas nigdzie opisany. Część zaleceń znajdziemy w podobnych opracowaniach dotyczących bezpieczeństwa. Niektóre z zaleceń są bowiem na tyle uniwersalne, iż będą miały zastosowanie, niezależnie do jakich odbiorców są skierowane.

16 Urządzenie NAS (Network Attached Storage) to serwer plików podobny do małego komputera, mający za zadanie przechowywanie danych. Jest wykorzystywane przez wielu małych i średnich przedsiębiorców, w tym kancelarie prawne. Na rynku znajdują się również urządzenia oferowane do użytku domowego.

 DOI: 10.54383/0031-0344.2024.01.9

Na ostateczny kształt *Dobrych praktyk* miało wpływ dopasowanie ich do sposobu, w jaki najczęściej wykonywany jest zawód przez profesjonalnych pełnomocników przy uwzględnieniu narzędzi służących w codziennej pracy.

Mając na uwadze powyższe, przy zapoznawaniu się z zaleceniami *Dobrych praktyk* warto zidentyfikować te z zaleceń, które będą znajdowały również podstawę w treści przepisów prawa i norm aktów samorządu adwokackiego. Zalecenia te należy bowiem rozważyć do wdrożenia jako wiążące, pomimo iż nie wynika to z charakteru *Dobrych praktyk*.

Przechodząc przez poszczególne regulacje prawne, należy w pierwszej kolejności zwrócić uwagę na Prawo o adwokaturze, a w szczególności art. 6 tej ustawy. Zgodnie z jego treścią adwokat zobowiązany jest do ochrony wszystkich informacji, jakie uzyskał w związku ze świadczeniem pomocy prawnej. Norma ta nie określa precyzyjnie, jakimi środkami powinno zostać wykonane to zobowiązanie przez adwokata. W odróżnieniu od zagrożeń dotyczących tradycyjnych form wykonywania zawodu, w przypadku cyberzagrożeń do ujawnienia informacji objętych tajemnicą adwokacką będzie zazwyczaj dochodziło w sposób nieumyślny. Tym samym w przypadku naruszenia art. 6 Prawa o adwokaturze w związku z incydentem cyberbezpieczeństwa oceniane będą podjęte działania i zaniechania oraz jaki miały wpływ na zaistniały incydent bezpieczeństwa.

Podkreślić należy, iż nie istnieją zabezpieczenia, które można ocenić jako w pełni skuteczne. Jedyną zatem formą zabezpieczenia się przed naruszeniem art. 6 Prawa o adwokaturze pozostaje wprowadzenie adekwatnych do zidentyfikowanego ryzyka sposobów zabezpieczania dostępu do informacji i przeciwdziałania sytuacjom, które mogą zwiększać zagrożenie. Odnosząc powyższe do niewiążącego charakteru *Dobrych praktyk*, należy stwierdzić, że brak ich stosowania nie może być podstawą do odpowiedzialności dyscyplinarnej, natomiast niestosowanie żadnego zabezpieczenia lub stosowanie takich, które nie są adekwatne do sposobu świadczenia pomocy prawnej lub prowadzenia działalności gospodarczej, może być oceniane negatywnie w przypadku, w którym doszłoby do ujawnienia informacji objętych tajemnicą adwokacką.

Zaleceniem *Dobrych praktyk*, którego zastosowanie będzie argumentem za wykazaniem, iż otrzymane przez adwokata informacje są chronione przed nieuprawnionym dostępem, będzie szyfrowanie. Dotyczy to zarówno szyfrowania przy przechowywaniu, jak i w komunikacji. Nie jest to oczywiście jedyne zalecenie, które należy wziąć pod uwagę, ale jedno z najbardziej oczywistych i uniwersalnych.

Bardziej szczegółowe normy w zakresie ochrony tajemnicy adwokackiej zostały wprowadzone w Kodeksie Etyki Adwokackiej, gdzie w § 19 określono już wprost zobowiązanie do zabezpieczenia przed ujawnieniem informacji objętych tajemnicą adwokacką. Dotyczy to każdego rodzaju dokumentów, niezależnie od miejsca przechowywania. Tym samym obowiązek stosowania zabezpieczeń istniał już przed uchwaleniem *Dobrych praktyk* w obowiązujących normach dotyczących obowiązków adwokatów.

DOI: 10.54383/0031-0344.2024.01.9

Sposób zabezpieczenia został pozostawiony do indywidualnej oceny. Wykazanie zatem, iż podjęte zostały kroki do zabezpieczenia informacji objętych tajemnicą adwokacką, może polegać na stosowaniu zaleceń określonych w *Dobrych praktykach*. Wskazanie, które zalecenia *Dobrych praktyk* powinny mieć zastosowanie, wymaga indywidualnej oceny ryzyka uwzględniającej rodzaje narzędzi i usług online wykorzystywanych w świadczeniu pomocy prawnej lub prowadzeniu działalności gospodarczej. W przypadku braku dostatecznego rozeznania przy dokonywaniu oceny ryzyka, równie dobrze można przyjąć założenie, iż zastosowanie wszystkich zaleceń dotyczących danego zakresu może być mocnym argumentem potwierdzającym zachowanie należytej staranności w zakresie stosowania zabezpieczeń (choć każdy przypadek naruszenia byłby oceniany indywidualnie).

Dalsze ustępy § 19 Kodeksu Etyki Adwokackiej pozwalają również na lepsze sprecyzowanie zakresu zobowiązań, wskazując między innymi na stosowanie oprogramowania zabezpieczającego przed niepowołanym ujawnieniem tajemnicy adwokackiej. Realizacja tego zobowiązania może polegać na stosowaniu zarówno oprogramowania zabezpieczającego przed cyberzagrożeniami, np. oprogramowania antywirusowego, jak i stosowaniu oprogramowania pochodzącego od zaufanych dostawców. Obie kategorie zaleceń znajdują się w *Dobrych praktykach*, tym samym stosowanie ich powinno być rozpatrywane przez pryzmat istnienia normy zobowiązującej do ich stosowania w Kodeksie Etyki Adwokackiej.

Do powyższej kategorii zaleceń dotyczących oprogramowania będzie należało również zalecenie *Dobrych praktyk* do korzystania z licencjonowanego i aktualnego oprogramowania przeznaczonego do komercyjnego zastosowania. Nie wynika to wprost z § 19 Kodeksu Etyki Adwokackiej, natomiast jest logicznym wnioskiem, popartym również praktyką. Wykazanie stosowania oprogramowania zabezpieczającego przed ujawnieniem tajemnicy adwokackiej będzie dostatecznie uzasadnione tylko w przypadku, gdy to oprogramowanie będzie spełniało funkcje, jakie są mu przypisywane. W tym celu musi być zatem aktualne, aby przeciwdziałać coraz nowym cyberzagrożeniom, licencjonowane, aby w ogóle móc powołać się na jego stosowanie, a także powinno być komercyjne, gdyż znaczna większość oprogramowania jest przystosowana do warunków i ryzyk odpowiadających celowi, jakiemu ma służyć. Często też brak możliwości stosowania niekomercyjnego oprogramowania do celów komercyjnych wynika wprost z treści samej licencji. Powyższe zalecenia stosowane łącznie nie niwelują całkowicie ryzyka, ale dają silne podstawy do uznania, iż usługa jest przygotowana do bezpiecznego korzystania. Natomiast nie można pominąć obowiązku każdorazowego zapoznania się z warunkami wykorzystywania danego oprogramowania przed jego uruchomieniem, a w szczególności przed wykorzystaniem do przesyłania tajemnicy adwokackiej.

 DOI: 10.54383/0031-0344.2024.01.9

W § 19 Kodeksu Etyki Adwokackiej zostało również określone zobowiązanie do informowania klienta o ryzyku przy korzystaniu m.in. z komunikatorów internetowych czy poczty elektronicznej. Zatrzymując się chwilę nad tym zaleceniem, w pierwszej kolejności należy wskazać, iż w celu poinformowania o ryzyku, najpierw należy je zidentyfikować i prawidłowo ocenić. Tym samym rekomendacja wynikająca z *Dobrych praktyk*, aby najpierw dokonać indywidualnej oceny ryzyka i dopiero do niej dostosować adekwatne zalecenia, ma swoje uzasadnienie także w normach obowiązujących adwokatów w przypadku korzystania z komunikacji elektronicznej.

Innym aktem samorządu adwokackiego regulującym sposób zabezpieczenia tajemnicy adwokackiej jest Regulamin. W § 5 ust. 1 Regulaminu określono normę zobowiązującą do postępowania z informacjami objętymi tajemnicą adwokacką w sposób uniemożliwiający zapoznanie się z nimi osobom nieuprawnionym. W akcie tym nie doprecyzowano wprost, jakimi metodami należy się posłużyć, ale z treści § 5 ust. 2 Regulaminu wynika, iż istotne jest identyfikowanie sytuacji, w których do takiego zapoznania mogłoby dojść, co dotyczy również pracowników kancelarii. Wśród zaleceń *Dobrych praktyk*, które mogą spełniać wymagania § 7 ust. 1 i 2 Regulaminu, jest stosowanie silnych haseł dostępowych, których założeniem jest uniemożliwienie dostępu do zabezpieczonych materiałów, a także stosowanie uwierzytelniania wieloskładnikowego (MFA), które wprowadza dodatkowe zabezpieczenie w przypadku przełamania hasła. Stosowanie tych zaleceń łącznie z zaleceniem do stosowania oddzielnych haseł do kont dostępowych będzie umożliwiało identyfikowanie, kto z pracowników kancelarii miał dostęp do określonych danych, a jednocześnie będzie stanowiło zabezpieczenie uniemożliwiające zapoznanie się z danymi osobom nieuprawnionym.

Kolejne zobowiązanie określone w § 5 ust. 3 Regulaminu wprost wskazuje na konieczność zabezpieczenia informacji przed utratą, zniszczeniem lub zniekształceniem. Stosowanie szeregu zaleceń dotyczących tworzenia kopii zapasowych określonych w *Dobrych praktykach* będzie w tym przypadku adekwatnym zabezpieczeniem pomagającym wykazać spełnienie tego zobowiązania. W zakres ten wchodzą zalecenia dotyczące wykonywania kopii zapasowych systemu operacyjnego i danych, wykonywania kopii zapasowych na urządzeniach zewnętrznych, niewykonywania kopii zawierających informacje objęte tajemnicą adwokacką na serwerach producentów smartfonów i dostawców telekomunikacyjnych, szyfrowania kopii, wykonywania dodatkowej kopii lokalnej, wykonywania kopii zawsze przed aktualizacją oprogramowania.

Oczywiście nie są to kompletne zalecenia, a jedynie przykłady. Natomiast fakt istnienia zobowiązań do określonego działania obliguje ich odbiorców do rozważenia stosowania zaleceń mieszczących się w tym zakresie i wybrania adekwatnych zarówno odnośnie do miejsca, jak i rodzaju dokumentów.

DOI: 10.54383/0031-0344.2024.01.9

Należy również podkreślić, iż forma i zakres zaleceń dotyczących cyberbezpieczeństwa mogą zmieniać się z czasem ze względu na treść wprowadzonego z początkiem tego roku nowego § 5 ust. 7 Regulaminu. Postanowienie to umożliwia wprowadzenie rekomendacji dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata w formie uchwał Naczelnej Rady Adwokackiej. Jest to rozwiązanie, które należy uznać za adekwatne ze względu na dynamiczny rozwój nowych technologii i powiązane z nim nowe formy cyberzagrożeń, a co za tym idzie – konieczność regularnej aktualizacji zabezpieczeń.

VII. Podsumowanie

Każdy z adresatów *Dobrych praktyk* powinien być świadomy zagrożeń związanych z wykorzystywaniem w działalności zawodowej infrastruktury informatycznej, w tym przetwarzaniem danych objętych tajemnicą zawodową w usługach dostarczanych drogą elektroniczną (w szczególności w usługach wykorzystujących chmurę obliczeniową). Dobre praktyki stanowią materiał pomocny w utrzymaniu cyberhigieny. Mając jednak na uwadze szybkie tempo zmian technologicznych oraz wzrastający poziom cyberzagrożeń, należy stwierdzić, że utrzymanie aktualnego charakteru *Dobrych praktyk* może nie być wystarczające. Naczelna Rada Adwokacka rozważa aktualizację tego dokumentu jeszcze w 2024 r. Rekomendujemy zatem również śledzenie aktualnych zaleceń instytucji zajmujących się tematyką cyberbezpieczeństwa (np. ENISA[17], NASK PIB CSIRT[18]).

Przemysław A. Barchan

Autor jest adwokatem (Izba Adwokacka w Warszawie), dyrektorem Instytutu LegalTech przy NRA, przewodniczącym zespołu ds. Dobrych praktyk dotyczących cyberbezpieczeństwa Instytutu LegalTech przy NRA, współautorem Dobrych praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata, wykładowcą Uniwersytetu SWPS.

The author is an advocate (District Bar Association in Warsaw), director of the Institute of LegalTech of National Bar Council, chair of the cybersecurity good practices team of the Institute of LegalTech of National Bar Council, co-author of the Cybersecurity good practices in law firms' operations and advocate's work, lecturer at SWPS University.

e-mail: pbarchan@barchan.pl

17 European Union Agency for Cybersecurity.

18 Computer Security Incident Response Team Państwowego Instytutu Badawczego NASK.

 DOI: 10.54383/0031-0344.2024.01.9

Piotr Warchoł

Autor jest adwokatem (Izba Adwokacka w Warszawie), wicedyrektorem Instytutu LegalTech przy NRA, członkiem zespołu ds. Dobrych praktyk dotyczących cyberbezpieczeństwa Instytutu LegalTech przy NRA, współautorem Dobrych praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata.

The author is an advocate (District Bar Association in Warsaw), vice director of the Institute of LegalTech of National Bar Council, member of the cybersecurity good practices team of the Institute of LegalTech of National Bar Council, co-author of the Cybersecurity good practices in law firms' operations and advocate's work.

e-mail: piotr.warchol@adwokatura.pl

Abstract

Keywords: *cybersecurity, advocate - client confidentiality privilege, good practices*

Cybersecurity good practices in law firms' operations and advocate's work – introduction

The ongoing digital transformation of the legal industry is an irreversible phenomenon that is conditioning law firms, regardless of their size. The aforesaid process carries a number of risks related to the security of the IT infrastructure and the security and confidentiality of the data held by an advocate. In the digital world, the protection of attorney-client privilege brings with it a number of challenges, not only of a legal, but also of a technical and organizational nature.

This article is a concise presentation of Good practices, which are one of the National Bar Council's responses to the increasing number of cyber threats and the need to raise awareness of cyber hygiene among the advocates' community.

DOI: 10.54383/0031-0344.2024.01.9

Bibliografia

Michał Duszczyk, *Polska jednym z kluczowych celów cyberprzestępców. Ataki rosną lawinowo*, „Rzeczpospolita", 5.01.2023 r.

https://www.rp.pl/biznes/art37728661-cyberataki-polska-liczba-cele

https://crn.pl/aktualnosci/hakerzy-coraz-czesciej-atakuja-w-polsce/

Raport LegalTech 2023, 31.03.2023 r., C.H. Beck,
https://legalis.pl/legaltech-raport-2023/

Raport The ENISA Threat Landscape (ETL) report, listopad 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

DOI: 10.54383/0031-0344.2024.01.9