

RAPPORT
LegalTech
2023



| C.H. BECK

legalis C.H.BECK

Komentarze C.H.Beck do wszystkich dziedzin prawa



Wejdź na konfigurator.legalis.pl
Kup online - korzystaj od razu!

Spis treści

Wstęp	2
Rozwiązania informatyczne z zakresu legal tech	4
Źródła wiedzy prawniczej	14
Obsługa informatyczna / Cyberzagrożenia w pracy prawnika	16
Sztuczna inteligencja a zawód prawnika	28
Media społecznościowe	34
Metryczka	36

Oddajemy w Państwa ręce tegoroczny raport dotyczący wykorzystania nowoczesnych technologii w pracy prawnika. Opracowanie opiera się na badaniu przeprowadzonym w styczniu 2023 roku na grupie 251 prawników. Ankietowani odpowiadali m.in. na następujące pytania: z jakich źródeł adwokaci i radcowie prawni czerpią informacje, czy i jakie narzędzia z zakresu legal tech wykorzystują w swojej codziennej pracy, na ile poszczególne obszary legal tech uważają za istotne dla rozwoju branży prawniczej.

Zapytaliśmy także o to, jakich zadań nie zastąpi sztuczna inteligencja oraz o próby cyberataku na kancelarie. Wyniki badań zostały omówione przez specjalistów zajmujących się prawem nowych technologii, w tym m.in.: dr Aleksandrę Auleytner, prok. Agnieszkę Gryszczyńską, r. pr. Artura Piechockiego, r. pr. Tomasza Zalewskiego. Eksperckie komentarze oraz artykuły merytoryczne poszerzają raport o wnikliwą analizę poszczególnych zagadnień.

Zapraszamy do zapoznania się z tegorocznym *Raportem LegalTech 2023*.

Przyspieszenie cyfryzacji prawników **WIDOCZNE, ALE NIE GWAŁTOWNE**



prof. Przemysław Polański
ALK, Wydawnictwo C.H.Beck

Systemy informacji prawnej to najważniejsze narzędzia legal tech w pracy prawnika, ale zauważalnie zwiększa się również rola innych tego typu narzędzi. Niestety, wraz z cyberrozwojem rośnie też liczba cyberzagrożeń.

Rok 2022 to pierwszy rok po pandemii COVID-19, która przyniosła widoczne przyspieszenie cyfryzacji pracy prawników omawiane w poprzednich dwóch edycjach raportu. W ostatnim roku trend ten uległ w pewnych obszarach dalszemu przyspieszeniu, co kontrastuje ze stereotypem prawników jako osób nastawionych do nowinek technologicznych konserwatywnie. Wystarczy wskazać na użytkowanie Portalu Informacyjnego Sądów Powszechnych, który wykorzystywany jest do e-doręczeń pism sądowych przez 94% prawników, czy na dominację drogi e-mailowej w komunikacji z klientami, aby zrozumieć, jak głębokiemu przeobrażeniu uległa codzienna praca prawnika w Polsce.

W ostatniej edycji raportu po raz kolejny zapytaliśmy prawników o rozumienie pojęcia legal tech. Tym razem większość respondentów wskazała na utożsamienie go z nowinkami technicznymi ułatwiającymi pracę prawnika, a jedynie 3% uznało, że ucieleśnienie tego pojęcia stanowią Legalis i Lex. To paradoks, biorąc pod uwagę fakt, że na pytanie o przykład narzędzia informatycznego w codziennej pracy respondenci wskazali właśnie na **systemy informacji prawnej jako na najważniejsze egzemplifikacje terminu legal tech**. Może to także oznaczać, że bazy wiedzy prawniczej nie są postrzegane jako najbardziej innowacyjne rozwiązania informatyczne na polskim rynku. Niemniej systemy informacji prawnej stanowią najważniejsze źródło wiedzy prawniczej istotne z punktu widzenia rozwoju zawodowego, na co wskazało blisko 90% respondentów.

Bez zaskoczenia należy jednak wskazać na stały już trend wskazujący na wagę podpisu cyfrowego w codziennej pracy prawnika w Polsce. Z darmowego Profilu Zaufanego na platformie ePUAP korzysta 80% prawników, natomiast z odpłatnych kwalifikowanych podpisów elektronicznych

niewiele mniej, bo aż 73% respondentów. **Ważnym trendem na rynku legal tech jest zauważalna już rola szeregu platform do automatyzacji procesu podpisywania i przechowywania umów.** Z komercyjnych platform do elektronicznego podpisywania i przechowywania umów, z których korzysta już ponad ¼ respondentów (27% w 2022 roku w stosunku do 16% w 2021 roku), w tym blisko ⅓ prawników zatrudnionych w przedsiębiorstwach oraz blisko połowa prawników pracujących w większych kancelariach prawnych. To charakterystyczny rys badań przeprowadzonych w tym roku – kancelarie częściej korzystają z systemów informacji prawnej, natomiast prawnicy in-house są dużo bardziej wymagający w odniesieniu do innowacyjnych rozwiązań z obszaru legal tech.

W ostatnim roku przyspieszyła także informatyzacja kancelarii prawnych w związku z wdrażaniem rozwiązań informatycznych do zarządzania kancelariami prawnymi. **Z narzędzi do zarządzania korzysta obecnie 29% kancelarii w stosunku do 19% w roku poprzednim, przy czym aż 37% rozważa wdrożenie tego typu narzędzi w najbliższym czasie.** Jeśli prognozy te się spełnią, może to oznaczać, że w przyszłorocznym raporcie ponad połowa kancelarii będzie dysponowała informatycznym narzędziem do wspomagania pracy prawników i zarządzania kancelarią. Tendencja do informatyzacji wewnętrznych procesów w kancelariach jest szczególnie widoczna w największych miastach, w których zaledwie mniej niż ¼ kancelarii w ogóle nie posiada ani nie planuje wdrożenia takiego narzędzia w najbliższej przyszłości.

Analizując odpowiedzi respondentów w obszarach dotyczących cyberbezpieczeństwa, należy podkreślić kolejny istotny trend, a mianowicie wzrost liczby ataków cybernetycznych na kancelarie prawne. **W 2022 roku aż 33% respondentów padło ofiarą ataków na infrastrukturę informatyczną, w tym ponad połowa większych kancelarii prawnych!** Jest to najwyższy niepokojący wynik na przestrzeni ostatnich czterech lat.

W 2022 roku
aż 33% respondentów
padło ofiarą ataków
na infrastrukturę
informatyczną, w tym
ponad połowa
większych kancelarii
prawnych!

Spośród cyberprzestępstw należy wskazać na trzy rodzaje cyberataków, z którymi muszą się liczyć kancelarie. Po pierwsze, *phishing*, czyli **podsywanie się przestępcy pod inną osobę lub instytucję mające na celu wyłudzenie informacji**. Dotyczył on **aż 57% kancelarii**. Z kolei ze złośliwym oprogramowaniem wykorzystanym do np. zaszyfrowania danych na dysku prawnika spotkało się 33% respondentów. Ataki polegające na blokowaniu infrastruktury poprzez atak typu *Denial of Service* dotknęło blisko co piątą pytaną kancelarię.

Podobnie jak w poprzednich latach do najpopularniejszych sposobów zabezpieczenia się kancelarii przed cyberatakiem należą: szyfrowanie danych (75%), cykliczna zmiana haseł (74%) oraz cykliczny back up danych (65%). **Niezmiennie zaskakuje, że ponad 1/3 kancelarii nie zabezpiecza swoich danych w postaci tworzenia kopii zapasowej plików**. Różnego rodzaju zabezpieczenia technologiczne przed cyberatakiem istotnie częściej stosowane są przez większe kancelarie, zatrudniające 4 lub więcej pracowników. Większe kancelarie polegają też częściej na outsourcingu usług informatycznych. Przechodząc do bardziej przyszłościowych tematów, a konkretnie do roli sztucznej inteligencji w pracy prawników, **zaledwie 5% respondentów przyznało się do korzystania z narzędzi wykorzystujących sztuczną inteligencję**. Widać wyraźnie, że prawnicy nie utożsamiają korzystania z bezpłatnych narzędzi, takich jak wyszukiwarka Google, jako korzystania z AI. Z pewnością jest też zbyt wcześnie, aby ocenić wpływ na pracę prawników przełomowych narzędzi, takich jak ChatGPT, które choć uruchomiono jeszcze w listopadzie 2022 roku, szerzej zaczęto je wykorzystywać dopiero na początku 2023 roku. Podobnie jak w poprzednich latach, prawnicy nie wykazują obecnie większych obaw przed narzędziami sztucznej inteligencji, wskazując, że AI nie zastąpi prawnika w przypadku niestandardowej sprawy czy w przypadkach wymagających kontaktu z klientem i udzielenia mu wsparcia psychologicznego.



ROZWIĄZANIA INFORMATYCZNE Z ZAKRESU LEGAL TECH

Rozumienie pojęcia **LEGAL TECH**

ROZWIĄZANIA Z OBSZARU LEGAL TECH
ważne w codziennej praktyce prawniczej

Ważność obszarów legal tech
dla **ROZWOJU BRANŻY PRAWNICZEJ**

Korzystanie z podpisu elektronicznego
oraz profilu zaufanego na **PLATFORMIE ePUAP**

Komunikowanie się z **SĄDEM**

Korzystanie z **NARZĘDZI INFORMATYCZNYCH**
do wspomagania pracy prawników i zarządzania
kancelarią

Obszary pracy prawnika z potencjałem
DO ZOPTYMALIZOWANIA LUB ZAUTOMATYZOWANIA

PRAGMATYZM

wygrywa z innowacyjnością



adw. Mikołaj Śniatała
Instytut LegalTech NRA,
Kancelaria Trzecki Śniatała

Technologia nie kreuje nowych potrzeb dla prawników. Technologia musi się dostosować do prawników, którzy z kolei nieustannie dostosowują się do otoczenia, w którym wykonują swój zawód. **Pragmatyzm wygrywa z innowacyjnością** – widać to doskonale po wynikach badań dotyczących legal tech, przeprowadzonych przez Kantar na zlecenie C.H.Beck.

Prawnicy wymagają, aby rozwiązania technologiczne ułatwiły im pracę. To najczęstsza odpowiedź na pytanie: „Czym dla Pana(i) jest i jak rozumie Pan(i) pojęcie legal tech?” To bardzo trafna obserwacja i ważna informacja dla producentów rozwiązań z obszaru legal tech.

Prawnicy oczekują, że rozwiązanie ułatwi im pracę tu i teraz. Oczekują sprawdzonych rozwiązań dla obszarów, które ich zdaniem wymagają optymalizacji.

Analizując wyniki odpowiedzi na pytania dotyczące rozwiązań z obszaru legal tech ważnych w codziennej praktyce prawniczej, znajdujemy potwierdzenie, że polski legal tech oparty jest o stabilne narzędzia umożliwiające pracę w ramach znanego prawnikom otoczenia i uzupełniające klasyczne procesy pracy prawnika. Wyszukiwanie wiedzy, zawieranie kontraktów i generowanie treści szablonowych umów, a także programy do zarządzania kancelarią to z perspektywy czasu pracy

prawnika koszty działalności. Przed erą legal tech prawnicy byli zmuszeni, szukając usprawnień w tych obszarach, rozbudować strukturę kancelarii. **Obecnie pracę asystentów i pracowników administracyjnych kancelarii prawnicy wspomagają technologią.** Co istotne, respondenci oceniają obecnie te obszary jako ważne w praktyce prawniczej, ale także oczekują, że głównie to te obszary będą nadal rozwijane przez dostawców technologii.

Co ciekawe, **widać dużą różnicę pomiędzy kancelariami prawnymi a prawnikami typu in-house** przy udzielaniu odpowiedzi, na pytanie, czy legal tech kojarzy się z nowością (różnica 15 punktów procentowych). Może się to wiązać z osobistymi odczuciami respondentów w kontakcie z legal tech i koresponduje to z zauważalnym większym w porównaniu do kancelarii prawnych zainteresowaniem legal tech wśród przedsiębiorców, dla których pracują prawnicy in-house.

Ciekawe jest to, że **rozwiązania technologiczne z obszaru legal tech oparte o zdalny dostęp i wykorzystanie Internetu do pracy nie są utożsamiane jako rozwiązanie z obszaru legal tech.** Wynika to z tego, że rozwiązania w tych obszarach są skalowane globalnie i kierowane do szerokiego grona odbiorców, nie tylko do branży prawnej. Pomimo to doskonale radzą sobie z zaspokajaniem potrzeb prawników.

Zdaniem respondentów, najbardziej ekscytujące wśród entuzjastów legal tech **rozwiązania oparte o sztuczną inteligencję (AI)** nie są postrzegane jako **najważniejsze dla rozwoju branży prawniczej.**

Wydaje się, że pragmatyczne podejście do nowości wśród prawników powoduje, że rozwiązania oparte o AI w pierwszej kolejności znajdą zastosowanie w innych obszarach gospodarki, a do branży prawnej trafią, gdy staną się sprawdzone i powszechnie akceptowalne, podobnie jak to się stało z wykorzystaniem Internetu w pracy prawnika.

Można zauważyć **rosnące zainteresowanie prawników obszarem legal tech i gotowość do używania udostępnionych przez ich otoczenie rozwiązań informatycznych.** Aktualna popularność podpisów elektronicznych wynika z faktu, że administracja państwowa wprowadziła e-usługi oparte o podpis elektroniczny, a następnie przedsiębiorcy docenili powszechność i dostępność tego rozwiązania. Prawnicy dostosowali się w tym zakresie do wymagań rynku. Zapowiadana informatyzacja wymiaru sprawiedliwości będzie kolejnym krokiem milowym do sukcesu rozwiązań z obszaru legal tech. Jestem pewny, że prawnicy wykorzystają nowe możliwości w swojej praktyce i będą oczekiwać od dostawców technologii usprawnień w coraz to szerszym obszarze swojej działalności.

Rozumienie pojęcia LEGAL TECH

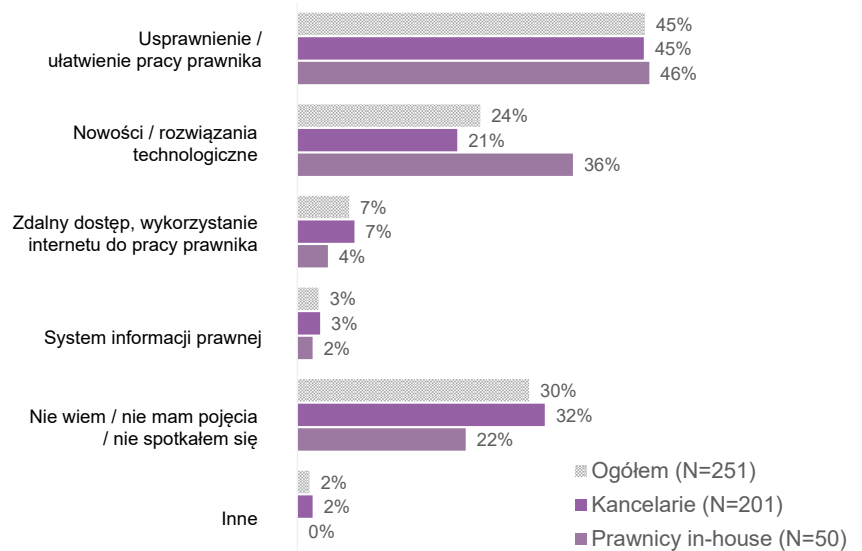
Najczęściej pojęcie legal tech kojarzy się z usprawnieniami, ułatwieniami w pracy prawnika (**45%**).

Co czwarty badany prawnik pojęcie to rozumie ogólnie – jako nowatorskie rozwiązania technologiczne.

Warto zauważyć, że nadal istnieje stosunkowo duża grupa prawników – **30%** (w 2021 roku – **43%**), którzy w ogóle nie zetknęli się z pojęciem legal tech.

Podstawa: wszyscy badani, N=251

Wykres 1. Czym dla Pana(i) jest i jak rozumie Pan(i) pojęcie „legal tech“?: PYTANIE OTWARTE

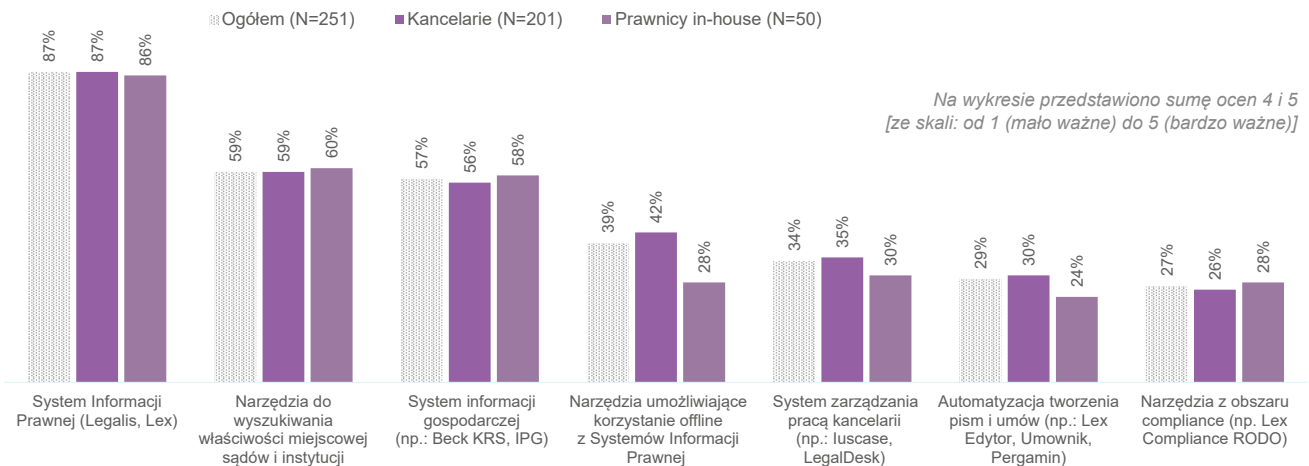


ROZWIĄZANIA Z OBSZARU LEGAL TECH ważne w codziennej praktyce prawniczej

Spośród rozwiązań informatycznych przeznaczonych dla prawników, za najważniejsze w codziennej pracy uznawane są Systemy Informacji Prawnej (**87%**).

Blisko **60%** prawników wysoko ocenia przydatność takich rozwiązań jak narzędzia do wyszukiwania właściwości miejscowej sądów i instytucji oraz systemy informacji gospodarczej.

Dla nieco ponad 1/3 prawników ważne w codziennej praktyce zawodowej są narzędzia umożliwiające korzystanie offline z systemów informacji prawnej oraz systemy zarządzania kancelarią; oba te rozwiązania istotnie częściej niż przeciętnie ważne są dla prawników z większych kancelarii – odpowiednio dla **53%** i **51%** z nich.



Podstawa: wszyscy respondenci; N=251

Wykres 2. Na ile różne rozwiązania informatyczne dla prawników (z obszaru legal tech) uważa Pan(i) za ważne w swojej codziennej praktyce?

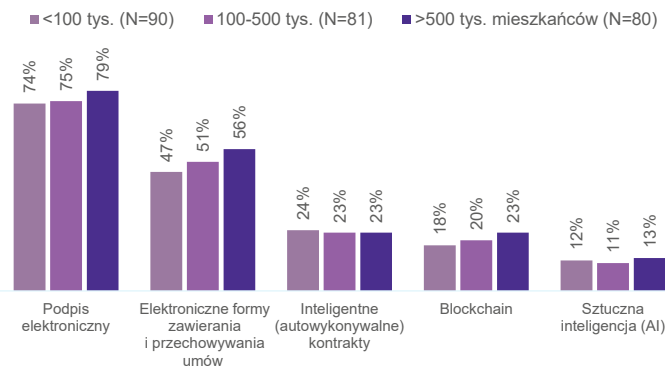
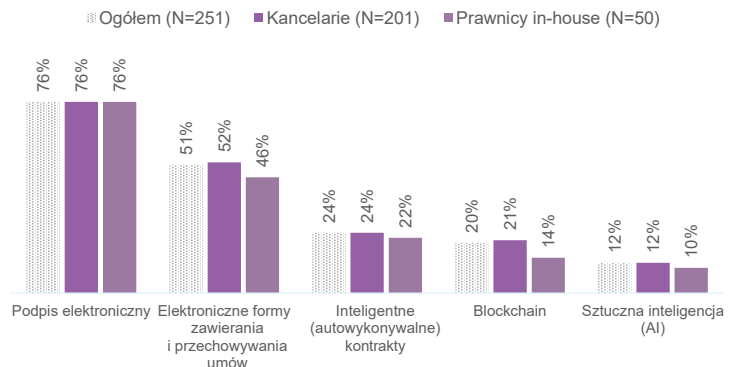
Ważność obszarów legal tech DLA ROZWOJU BRANŻY PRAWNICZEJ

Za najważniejszy obszar legal tech, w kontekście rozwoju branży prawniczej, uznawany jest podpis elektroniczny – uważa tak **76%** badanych prawników.

Elektroniczne formy zawierania i przechowywania umów uznawane są za istotne dla rozwoju branży przez co drugiego badanego prawnika.

Pozostałe obszary legal tech, o które pytano – inteligentne kontrakty, *blockchain* czy AI – rzadziej uznawane są za ważne.

Na wykresach przedstawiono sumę ocen 4 i 5 ze skali: od 1 (mało istotny) do 5 (bardzo istotny)



Podstawa: wszyscy respondenci; N=251

Wykres 3. Na ile poszczególne obszary legal tech uważa Pan(i) za istotne dla rozwoju branży prawniczej?



mec. Tomasz Zalewski
Bird&Bird,
Fundacja LegalTech
Polska

Raport LegalTech 2023 potwierdza moją opinię na temat poziomu stosowania rozwiązań legal tech przez polskich prawników:

- Podchodzą oni do tych rozwiązań bardzo pragmatycznie; w legal tech widzą przede wszystkim **wsparcie w codziennych czynnościach związanych ze świadczeniem pomocy prawnej**, takich jak uzyskiwanie wiedzy o prawie, o stanie sprawy sądowej, ustalanie właściwości miejscowej sądów i instytucji, rejestracja czasu pracy i rozliczenia, zarządzanie kancelarią.
- Nie dziwi zatem także popularność **podpisu elektronicznego**, który stał się narzędziem wykorzystywanym przez prawie wszystkich prawników (w 2022 r. aż 73% prawników ma podpis kwalifikowany, podczas gdy w 2021 r. miało taki podpis 52%). Tak duży skok w liczbie użytkowników kwalifikowanego podpisu elektronicznego świadczy o tym, że ten rodzaj podpisu stał się częścią standardowego zbioru narzędzi każdego prawnika.
- **Bardzo powoli, ale systematycznie rośnie grono użytkowników narzędzi automatyzujących** tworzenie pism i umów oraz narzędzi z zakresu compliance.
- **Polscy prawnicy sceptycznie podchodzą do narzędzi wykorzystujących sztuczną inteligencję** – używa ich wąska grupa prawników, a większość uważa, że narzędzia te w żaden sposób nie zagrażają sposobowi wykonywania przez nich zawodu.

Pozwala to na sformułowanie tezy, że **większość prawników w Polsce wykonuje zawód w sposób tradycyjny, a rewolucja technologiczna legal tech wywarła wpływ głównie na większe kancelarie oraz w zakresie sposobu działania kancelarii od strony administracyjnej**. W zasadzie jedynym przejawem stosowania legal tech przez prawników, który mogą dostrzec klienci, jest stosowanie podpisu elektronicznego.

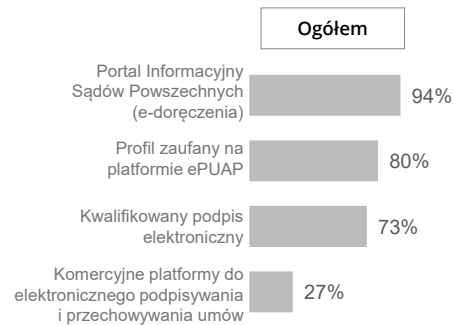
Niewątpliwie ciekawą informacją jest to, że **aż 1/3 prawników osobiście zetknęła się z próbami cyberataku**. Widać także wyraźnie, że **najmniej przygotowani do stawienia czoła zagrożeniom cyberbezpieczeństwa są prawnicy wykonujący zawód indywidualnie, co jest wskazówką dla samorządów odnośnie do kierunków edukacji w tym zakresie**.

Na tym tle zaskoczeniem jest wzrostowy trend liczby prawników korzystających z bezpłatnej poczty elektronicznej w chmurze. Oznacza to, że nadal wielu prawników nie rozumie, w jaki sposób działają bezpłatne usługi chmurowe oraz zapewne nie zdaje sobie sprawy z zagrożeń dla tajemnicy zawodowej. To wydaje się kolejnym ważnym zagadnieniem, na które trzeba zwrócić uwagę w edukacji prawników.

Korzystanie z podpisu elektronicznego oraz profilu zaufanego na **PLATFORMIE ePUAP**

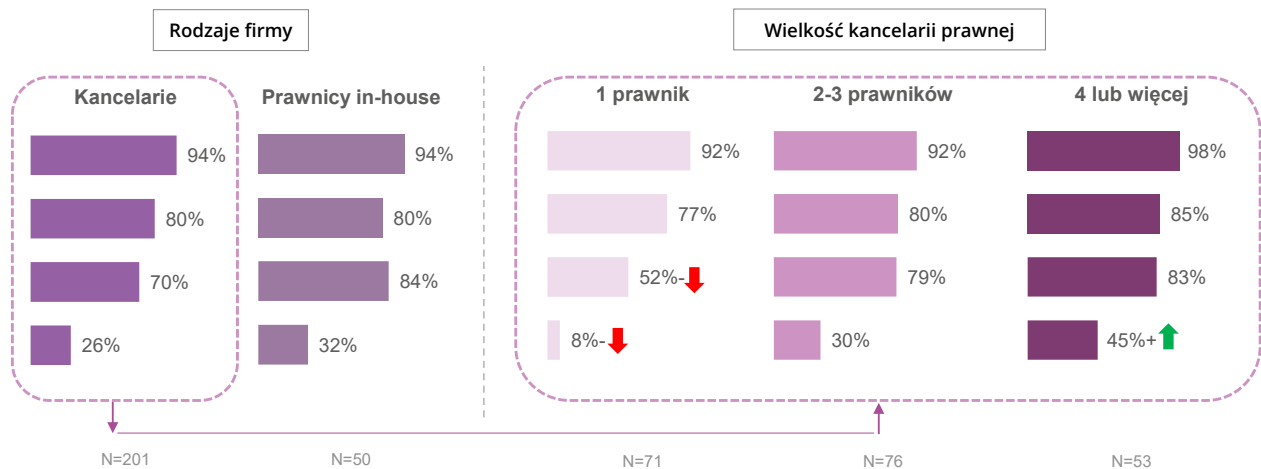
Z Portalu Informacyjnego Sądów Powszechnych (e-doręczenia) korzystają prawie wszyscy prawnicy (**94%**).

Z profilu zaufanego na platformie ePUAP korzysta, w ramach pracy zawodowej, **80%** prawników.



Kwalifikowanym podpisem elektronicznym posługuje się, w celach zawodowych, **73%** prawników, częściej – prawnicy in-house (**84%**).

Z komercyjnych platform do elektronicznego podpisywania umów korzysta nadal stosunkowo niewielu prawników (**27%**), jednak odsetek użytkowników tego narzędzia rośnie (w 2022 r. – **16%** prawników).



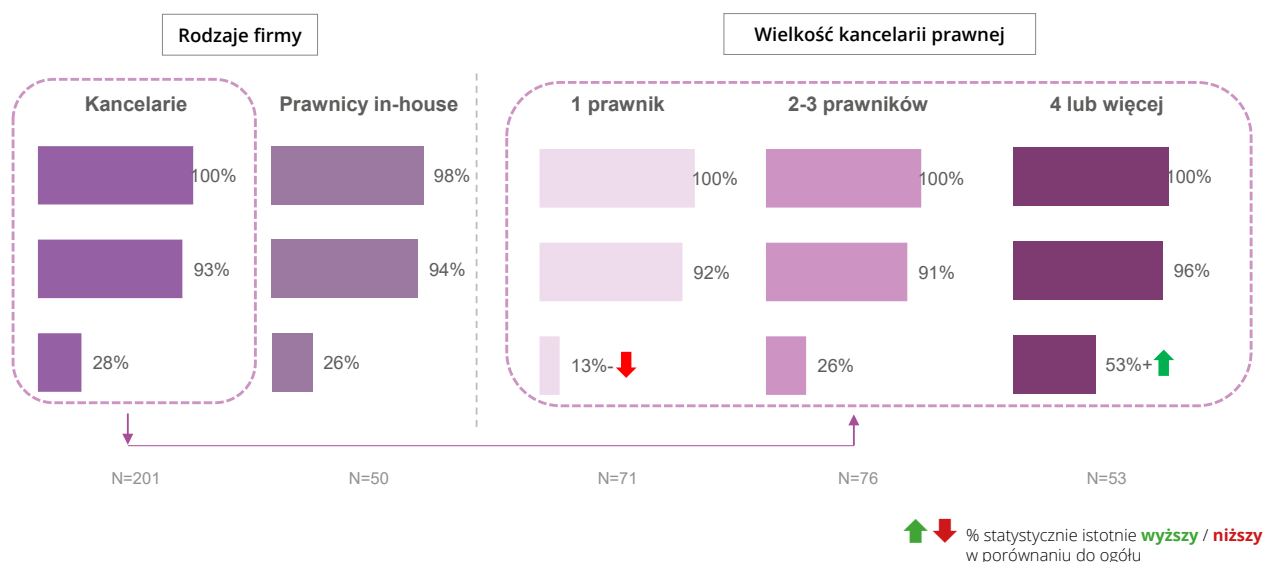
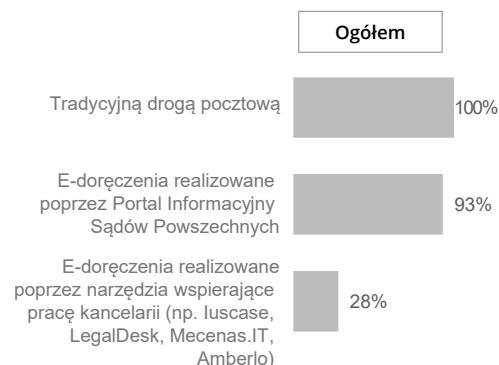
↑ ↓ % statystycznie istotnie **wyższy** / **niższy** w porównaniu do ogółu

Podstawa: wszyscy respondenci; N=251

Wykres 4. Czy wykorzystuje Pan(i) w swojej praktyce zawodowej...

Komunikowanie się Z SĄDEM

W sprawach, w których pojawia się konieczność komunikacji z sądem przez wszystkich stosowana jest komunikacja tradycyjną drogą pocztową; powszechną formą jest również e-doręczenie poprzez Portal Informacyjny Sądów Powszechnych (korzysta z niej **93%** prawników); e-doręczenia realizowane poprzez narzędzia wspierające pracę kancelarii, takie jak np. Iuscase, LegalDesk czy Mecenas.IT, generalnie niezbyt popularne (**28%**), istotnie częściej wykorzystywane są przez większe kancelarie (**53%**).



Podstawa: wszyscy respondenci; N=251

Wykres 5. W razie konieczności komunikacji z sądem odbywa się ona w Pan(i) przypadku poprzez:



r. pr. Witold Chomiczewski
Lubasz i Wspólnicy

Legal Tech jako narzędzie przewagi konkurencyjnej

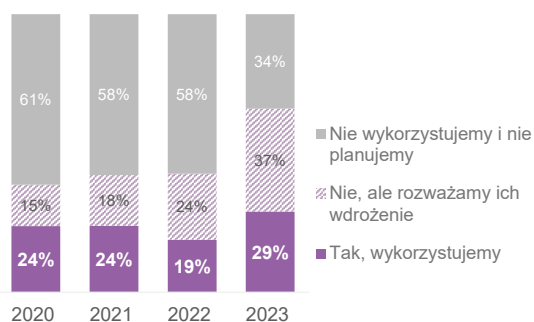
Raport pokazuje, jak duża jest jeszcze przestrzeń dla rozwoju rozwiązań legal tech. Sami prawnicy wskazują na obszary, w których automatyzacja procesów byłaby pożądana, np. analityka efektywności pracy czy analiza dokumentów. Jednocześnie sporym wyzwaniem jest **budowanie świadomości** zarówno samych rozwiązań legal tech wśród prawników, jak i korzyści wynikających z wykorzystania tych narzędzi. 30% badanych bowiem nadal nie spotkała się z pojęciem legal tech.

Osobiście zainteresowało mnie w wynikach, że choć 87% prawników uważa systemy informacji prawnej za ważny element w codziennej praktyce, to rozwiązania przeznaczone do automatyzacji tworzenia pism i umów są uważane za istotne tylko przez 29% badanych. To pokazuje, jak dużą **przewagę konkurencyjną** mogą osiągnąć ci prawnicy, którzy wcześniej zaczną wdrażać takie narzędzia.

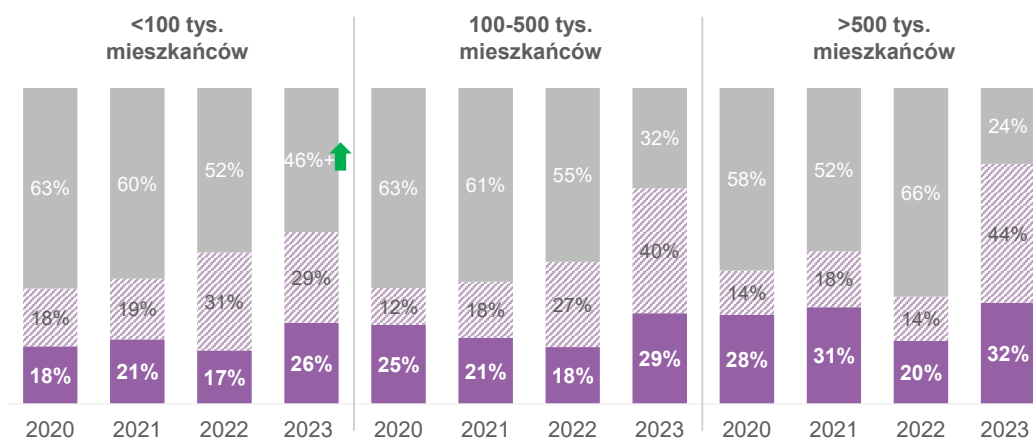
Korzystanie z **NARZĘDZI INFORMATYCZNYCH** do wspomaganie pracy prawników i zarządzania kancelarią

Korzystanie z narzędzi informatycznych do wspomaganie pracy prawników oraz zarządzania kancelarią rośnie i dotyczy obecnie **29%** prawników z kancelarii; rośnie również odsetek prawników rozważających korzystanie z takich narzędzi (**37%**).

Narzędzia te istotnie częściej wykorzystywane są przez prawników pracujących w największych miastach oraz prawników z większych kancelarii.



Wielkość miejscowości



↑ ↓ % statystycznie istotnie **wyższy** / **niższy** w porównaniu do ogółu

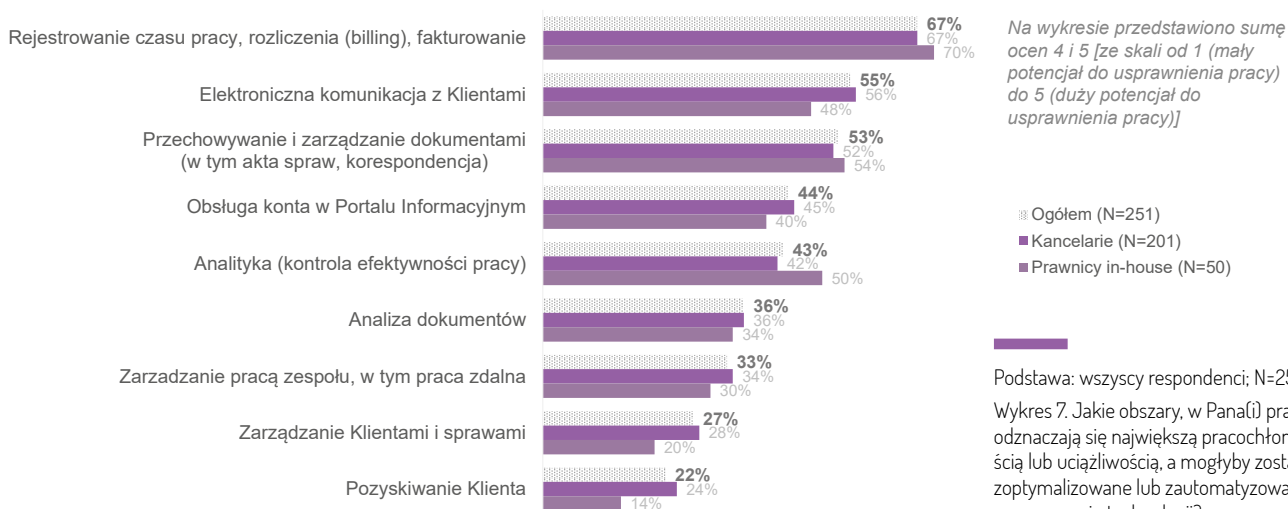
Podstawa: Kancelarie; 2020 r. N=202; 2021 r. N=202; 2022 r. N=200; 2023 r. N=201

Wykres 6. Czy w Pana(i) kancelarii wykorzystywane są narzędzia informatyczne do wspomaganie pracy prawników i zarządzania kancelarią, takie jak np. Iuscase, Kleos, LegalDesk, Mecenase.IT, lub rozważacie Państwo ich wdrożenie?

Obszary pracy prawnika z **POTENCJAŁEM** do zoptymalizowania lub zautomatyzowania

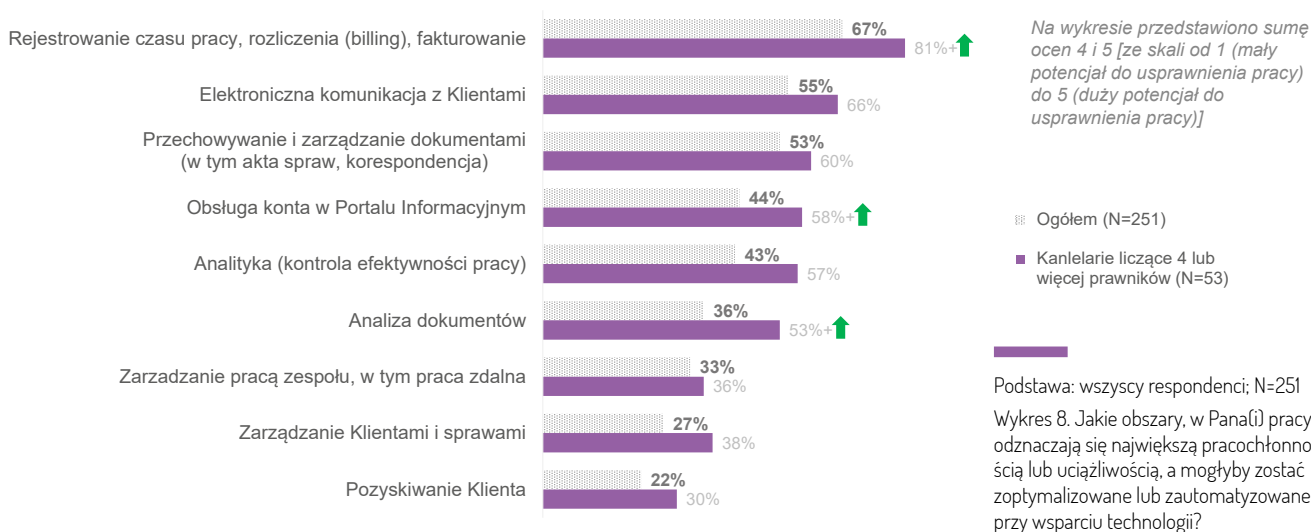
Obszary pracy, które, zdaniem prawników, są pracochłonne i jednocześnie mają największy potencjał usprawnienia dzięki rozwiązaniom technologicznym to:

- rejestrowanie czasu pracy, rozliczenia, fakturowanie (**67%**),
- elektroniczna komunikacja z klientami (**55%**),
- przechowywanie i zarządzanie dokumentami, w tym akta spraw, korespondencja (**53%**).



Podstawa: wszyscy respondenci; N=251
Wykres 7. Jakie obszary, w Pana(i) pracy, odznaczają się największą pracochłonnością lub uciążliwością, a mogłyby zostać zoptymalizowane lub zautomatyzowane przy wsparciu technologii?

Prawnicy z większych kancelarii istotnie częściej niż przeciętnie dostrzegali wiele różnych pracochłonnych obszarów, które mogłyby zostać zoptymalizowane przy wsparciu technologii.



Podstawa: wszyscy respondenci; N=251
Wykres 8. Jakie obszary, w Pana(i) pracy, odznaczają się największą pracochłonnością lub uciążliwością, a mogłyby zostać zoptymalizowane lub zautomatyzowane przy wsparciu technologii?

LEGAL TECH jest nadal w blokach startowych!



r. pr. Mikołaj Otmianowski
DAPR

Dla kreatywnych prawników to dobrze, bo stają się liderami rynku. Dużo się mówi i sporo się tworzy w zakresie legal tech w Polsce. Choć dużo mówi się, ale tylko w określonych kręgach podążających za nowymi rozwiązaniami. Prawniczy świat legal tech w Polsce to zapewne około 100 prawników tworzących różne rozwiązania i kolejnych 1000 osób pasjonujących się i próbujących wykorzystać narzędzia legal tech w swojej pracy. Cała reszta branży nie jest nim zainteresowana. **W raporcie można przeczytać, że 30% prawników wciąż nie słyszało o legal tech.**

Legal tech to bieg długodystansowy,
a my ciągle tkwimy w blokach
startowych.

Prawnicy gremialnie rozumieją legal tech jako wyszukiwarki informacji, czyli bardzo podstawowe narzędzia do pracy. A także te narzędzia, z których realnie korzystają, czyli dostęp do sądu z wykorzystaniem aplikacji WEB, dostęp do informacji prawnej typu Legalis. Dobrze, że w raporcie wśród rozwiązań legal tech nie widnieją już Zoom, Teams ani inne programy pakietu Office. Kiedyś widziałem opracowania, które wskazywały na takie „legaltechowe” rozwiązania.

Nareszcie się to stało – **wysoki odsetek osób wykorzystuje kwalifikowany podpis elektroniczny**. Podpis ten przebił się przez wiele lat i można powiedzieć, że końcu wszedł na rynek. Aż dziw, że dostawcy tej usługi biznesowo „dożyli” tego momentu. A sam podpis to olbrzymie ułatwienie w obrocie gospodarczym!

Największe zaskoczenie. **Prawnicy dezawuuują istotność AI dla rozwoju branży**. Zważywszy na sukces czatu GTP, około 10 respondentów uważających AI jako istotny obszar dla rozwoju branży to zaskakująco słaby wynik. Jako grupa zawodowa nie powinniśmy być jak Jaś Fasola, który, odwracając głowę, myślał, że staje

się niewidzialny dla otoczenia. Osobiście uważam, że to jest szansa na przetasowanie w branży.

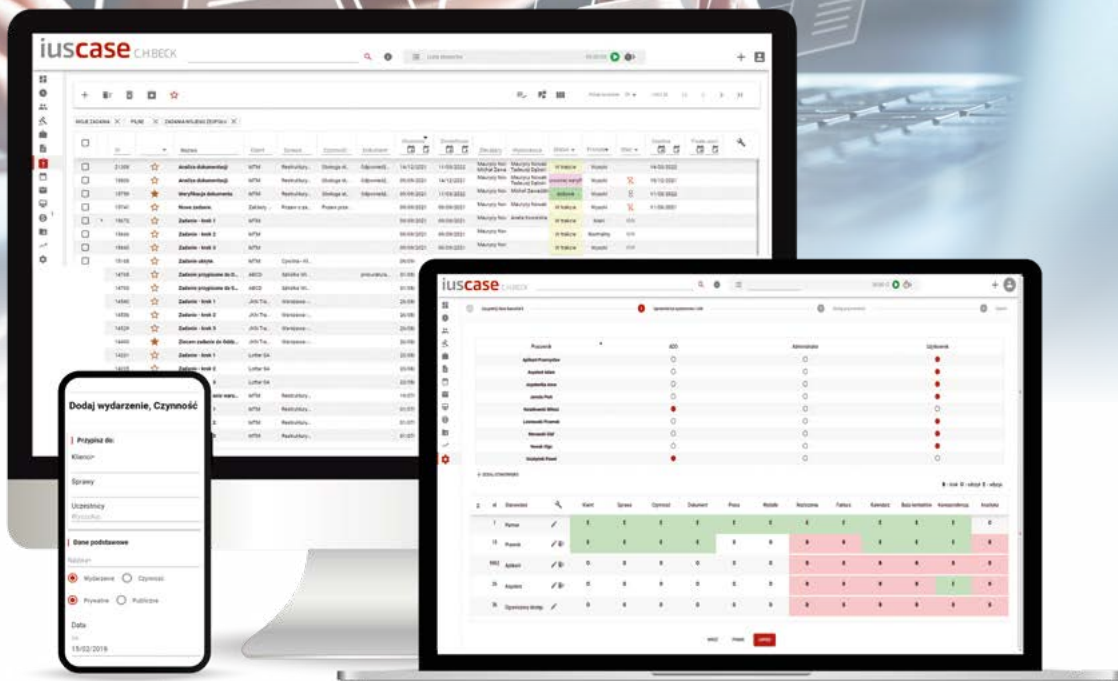
No i mój konik – rejestracja czasu pracy. To jest *never ending story*. Narzędzi sporo, wszyscy mają problem z notowaniem i przygotowywaniem raportów, ale nic z tym nie robią. Dla mnie to *must have*, bo **dobry system bieżącego notowania zadań to o 30% więcej przychodu dla kancelarii bez dodatkowych klientów**.

Wystarczy notować na bieżąco, bo:

- notujemy czas realny w pełnej wysokości,
- nie pomijamy żadnych czynności,
- możemy dostarczyć zestawienie klientowi przed innymi – kiedy budżet jest pełen i łatwiej zaakceptować pierwsze wydatki.

Z rejestracją czasu pracy ściśle wiąże się temat usprawnienia pracy prawnika, przez co rozumiem **stosowanie narzędzi pomagających sortować bazę wiedzy**. Narzędzi typu DMS. Transfer wiedzy i rozwój firmy bez tych narzędzi jest właściwie niemożliwy. **Przy takiej inflacji przepisów prawa trzeba regularnie porządkować dokumenty** i umożliwić ich odnalezienie innym osobom w zespole. Ostatnio pomyślałem, że warto zatrudnić bibliotekarza.

Podsumowując, patrząc na wyniki raportu, widzę pewną rozbieżność: myślimy *Legal tech to nowoczesność i sprawność*, a tymczasem w praktyce to narzędzia używane do wyszukiwania informacji. Sporo przed nami! Ze swojej strony zachęcam do testowania rozwiązań tworzonych dla prawników, bo to ważne zarówno dla rozwoju produktów legal tech, jak i dla samych prawników z nich korzystających, ponieważ sprawne wykorzystanie narzędzi może im dać przewagę konkurencyjną.



iuscase
C.H.BECK

Zarządzanie kancelarią prawną w jakości C.H.Beck

- iuscase to nowoczesny program do zarządzania kancelarią prawną powstały w oparciu o 30-letnie doświadczenie C.H.Beck na polskim rynku.
- **Zintegrowany z Portalem Informacyjnym Sądów Powszechnych.**
- Gwarantuje **kontrolę nad odbieraniem e-doręczeń** sądowych – moment ich otwarcia zależy od użytkownika.

Wypróbuj bezpłatnie

Zadzwoń **22 311 22 22** lub wejdź na **iuscase.pl**



C.H.BECK



ŹRÓDŁA wiedzy prawniczej

Waga różnych **zasobów wiedzy
prawniczej** istotnych z punktu
widzenia rozwoju zawodowego

Waga różnych zasobów wiedzy prawniczej istotnych z punktu widzenia rozwoju zawodowego

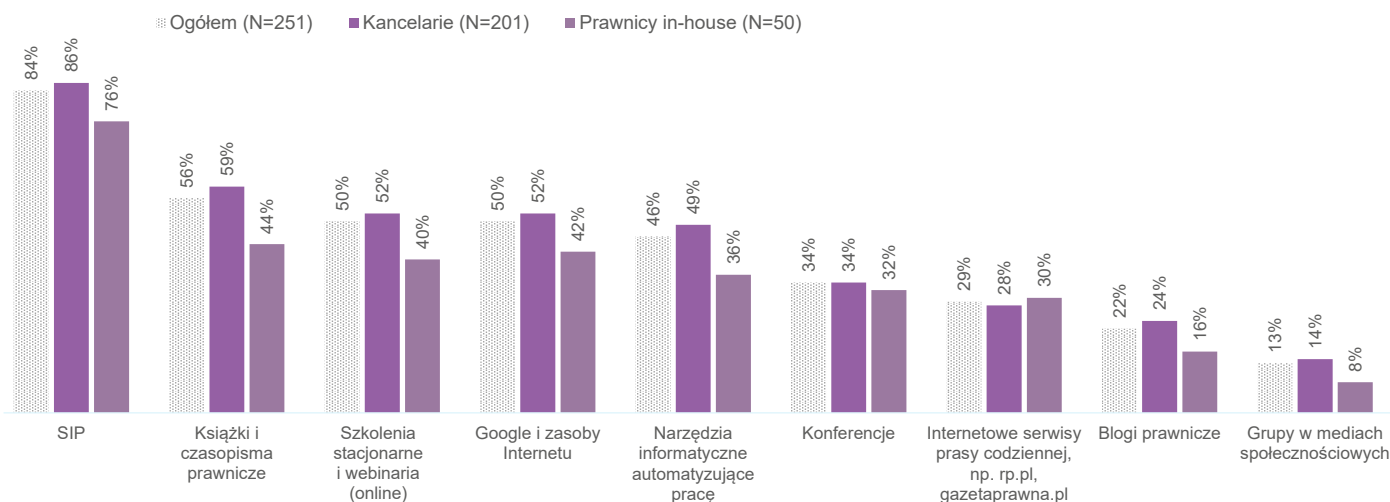
(84%) Spośród dostępnych zasobów wiedzy, zdecydowana większość prawników za ważne, dla swojego rozwoju zawodowego, uznaje Systemy Informacji Prawnej (84%).

(56%) Ważnymi zasobami wiedzy dla znacznej części prawników są również tradycyjne źródła, jakimi są książki prawnicze (56%).

(50%) Co drugi prawnik za ważne dla siebie uznaje szkolenia – stacjonarne i online.

(50%) (46%) Z nowoczesnych zasobów informacji najwięcej prawników ceni sobie Google i zasoby internetu (50%) oraz narzędzia informatyczne automatyzujące pracę (46%).

Na wykresie przedstawiono sumę ocen 4 i 5 [ze skali: od 1 (mało ważne) do 5 (bardzo ważne)]



Podstawa: wszyscy respondenci; N=251

Wykres 9. Na ile poszczególne zasoby wiedzy prawniczej, jakie odczytam, uważa Pan(i) za ważne dla swojego rozwoju zawodowego?

+5 満員

EP-1348543KJ

RF-FDFRBB3KJ

DV-23534FKJ

enter

main

EP/011

ACTIVE PRT

01
05

OBSŁUGA INFORMATYCZNA CYBERZAGROŻENIA W PRACY PRAWNIKA CHMURA

Sposób **ZORGANIZOWANIA
OBSŁUGI INFORMATYCZNEJ**
w kancelarii

DOŚWIADCZENIE związane
z próbami cyberataku

Sposoby zabezpieczenia
kancelarii przed **CYBERATAKIEM**

KOMUNIKACJA kancelarii z klientami

Korzystanie z otwartych
środowisk **CLOUDOWYCH**

-74.0059731	-40.7143528
-82.034345	-53.2553434
-91.234554	-65.3453455
-101.23245	-72.4354556

XO	10/0056
TE	21/6456
GH	52/3426
OP	72/3436
OTHER	94/3246

CYBERZAGROŻENIA w pracy prawnika



Marek Laskowski
Domański, Zakrzewski, Palinka

Podobnie jak w latach ubiegłych, wyniki badania cyberzagrożeń w pracy prawnika pokazują nieustająco **rosnące ryzyko cyberataków skierowanych na kancelarie prawne**.

Stosowane wektory ataków nie uległy znaczącemu przeobrażeniu – nadal jest to *phishing*, niemniej jednak skala i jakość tych ataków uległa widocznej zmianie.

W kontekście jakościowym **stosowany obecnie *phishing* ma charakter bardzo zaawansowany**, nazywany przeze mnie „**uwiarygadnianym**”. Oznacza to, że etap prostego spreparowanego e-maila, którego otwarcie skutkuje zainfekowaniem stacji lub całego środowiska IT, mamy już za sobą. Obecnie działania takie w wielu przypadkach są celowane i poprzedzane długim okresem kontaktu z potencjalnym celem, jakim jest prawnik czy dana kancelaria. Działania te są również zorientowane na pozyskanie konkretnych informacji (np. związanych z określoną usługą). Po okresie takiego dłuższego kontaktu osoba będąca adresatem wiadomości jest bardziej skłonna zaufać korespondencji pochodzącej od znanej jej osoby, co powoduje większą skuteczność ataku. Jednak nawet wobec tego typu zaawansowanych działań istnieją obecnie rozwiązania techniczne, które potrafią ograniczyć ich potencjalny negatywny wpływ na organizację. Dostrzegamy, że świadome kancelarie i prawnicy starają się je wdrażać.

Drugim istotnym wektorem ataku jest *malware*. Badanie pokazuje, jaka jest świadomość zagrożeń wynikających z tego zjawiska wśród prawników, niemniej jednak nadal pokutuje przekonanie, że odpowiedzią na *malware* jest stosowanie systemu antywirusowego. Jest to błędne przekonanie, które może skutkować problemami w przypadku zainfekowania *malwarem* czy *ransomwarem* itp. organizacji. Rekomendacje w tym zakresie od lat są podobne. Otóż **należy odchodzić od sygnaturowych systemów ochrony na rzecz zaawansowanych systemów, potrafiących wykrywać i reagować**

na ataki niesygnaturowe zarówno na poziomie serwerów, jak i stacji roboczych.

Dodatkowym wskazaniem może być wykorzystywanie **usług typu SOC** (*security operation center*) realizowanych przez wyspecjalizowane podmioty. Jednak należy w tym przypadku bardzo dokładnie przeanalizować oferty takich dostawców pod kątem skuteczności i szybkości reagowania na cyberincydenty.

Zmianie nie uległ również **cel cyberprzestępców atakujących kancelarie**. Z perspektywy zgromadzonych danych – firmy te są krytycznym ogniwem gospodarki, gdyż wycieki danych wrażliwych wielu kluczowych firm zgromadzonych w jednym miejscu mogłyby spowodować nieprzewidywalne negatywne skutki. Aktualny pozostaje również cel ataków, jakim jest zaszyfrowanie danych kancelarii i wymuszenie okupu.

Odnosnie do **cyberzabezpieczeń stosowanych przez kancelarie**, również niewiele się zmienia, a więc szyfrowanie danych i plików nadal stosowane jest powszechnie i uznawane za bezpieczne. Bez wątplenia szyfrować dane należy, ale jest to tylko jeden z elementów całego złożonego systemu ochrony, jaki kancelarie powinny wdrożyć. Napawa jednak optymizmem wzrost wśród prawników świadomości cyberbezpieczeństwa, ale także wartości danych, jakie posiadają kancelarie, oraz konieczności ich należytego zabezpieczenia.

Kancelarie wdrażają wiele technologii w zakresie ochrony danych, ale mam wrażenie, że nadal robią to w sposób wybiórczy i chaotyczny, bez zdefiniowania strategii takich działań. Badania pokazują, że **jesteśmy jako branża prawna nadal w procesie transformacji cyfrowej**, szczególnie w obszarze technologii dotyczących cyberochrony. Trend jest pozytywny, niemniej jednak w porównaniu z innymi sektorami gospodarki mamy jeszcze wiele do zrobienia.

Sposób zorganizowania OBSŁUGI INFORMATYCZNEJ w kancelarii

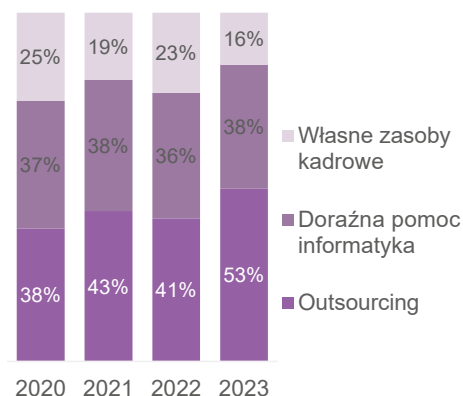
Obsługa informatyczna w kancelariach prawnych najczęściej zorganizowana jest na zasadzie outsourcingu (**53%**).

Drugie pod względem popularności rozwiązanie, oparte na dorażnej pomocy informatyka (**38%**), istotnie częściej stosowane jest w firmach w mniejszych miastach (**50%**) oraz w kancelariach zatrudniających 1 prawnika (**63%**).

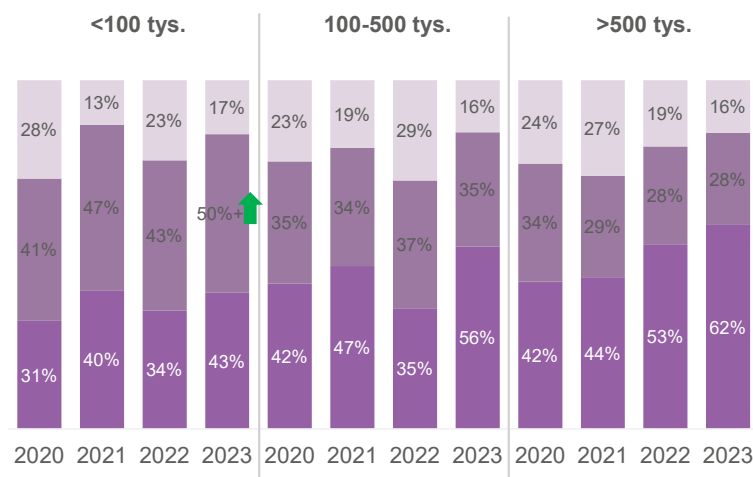
Najmniej popularny sposób obsługi informatycznej (własne zasoby kadrowe), dotyczący ogółem **16%** kancelarii, istotnie częściej ma miejsce w większych kancelariach (**36%**).

Podstawa: Kancelarie; 2020 r. N=202; 2021 r. N=202; 2022 r. N=200; 2023 r. N=201
Wykres 10. W jaki sposób organizowana jest w Pana(ł) kancelarii obsługa informatyczna?

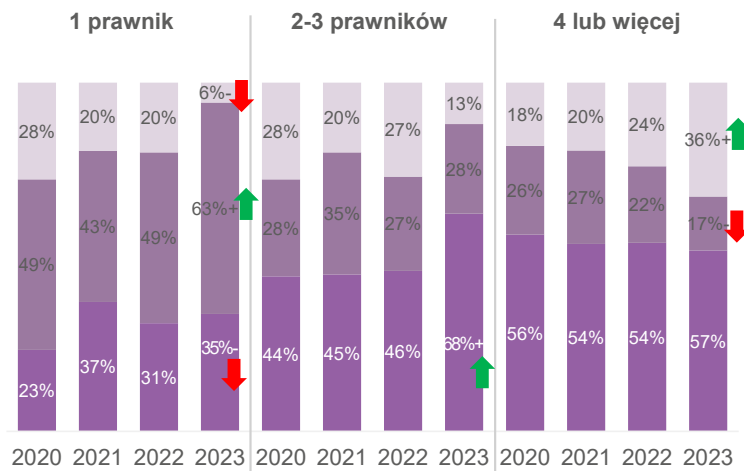
Kancelarie ogółem



Wielkość miejscowości



Wielkość kancelarii prawnej



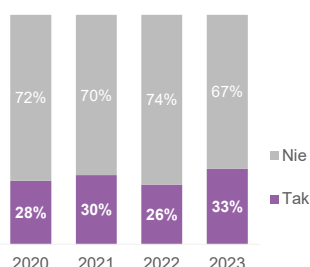
↑ ↓ % statystycznie istotnie wyższy / niższy w porównaniu do ogółu

Doświadczenie związane z próbami **CYBERATAKU**

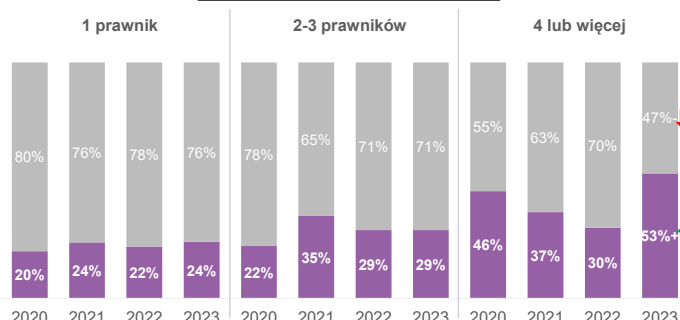
W tegorocznym pomiarze **33%** kancelarii przyznało, że zetknęło się z próbami cyberataku. Jest to najwyższy wynik na przestrzeni ostatnich czterech lat.

Cyberataki istotnie częściej zdarzają się w większych kancelariach, zatrudniających 4 lub więcej prawników (**53%**).

Kancelarie ogółem



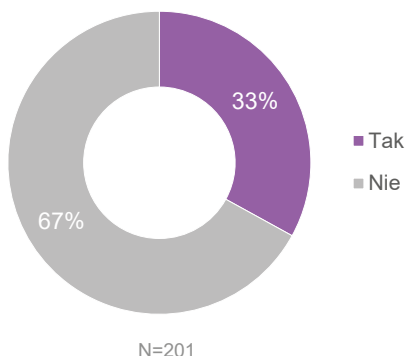
Wielkość kancelarii prawnej



↑ ↓ % statystycznie istotnie **wyższy** / **niższy** w porównaniu do ogółu

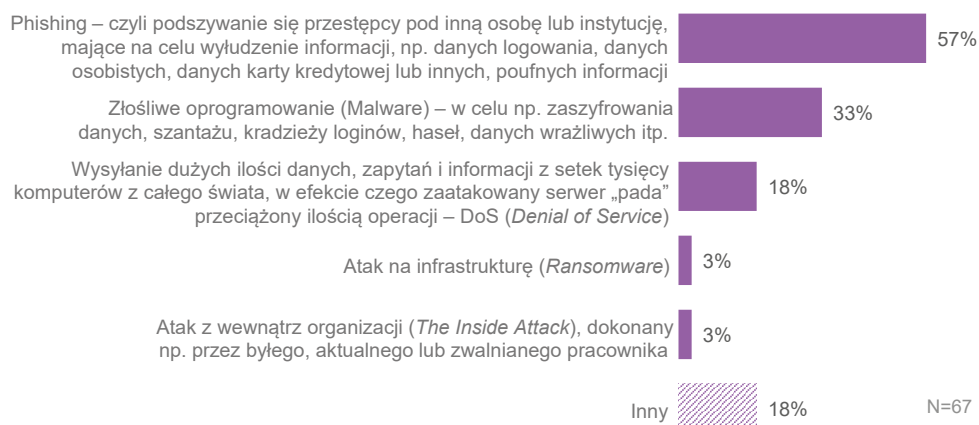
Podstawa: Kancelarie; 2020r. N=202; 2021 r. N=202; 2022 r. N=200; 2023 r. N=201
Wykres 11. Czy spotkał(a) się Pan(i) w swojej kancelarii z próbami cyberataku?

Kancelarie ogółem



Prawnicy, którzy zetknęli się w pracy z próbami cyberataku, najczęściej doświadczali problemów związanych z podszywaniem się przestępcy pod inną osobę lub instytucję w celu wyłudzenia poufnych danych (**57%**); w drugiej kolejności doświadczano problemów związanych ze złośliwym oprogramowaniem (**33%**).

Rodzaje doświadczanych prób cyberataku



Podstawa: Kancelarie; N=201
Wykres 12. Czy spotkał(a) się Pan(i) w swojej kancelarii z próbami cyberataku?
Wykres 13. Czego dotyczyła ta próba ataku?

CYBERZAGROŻENIA w branży prawnej

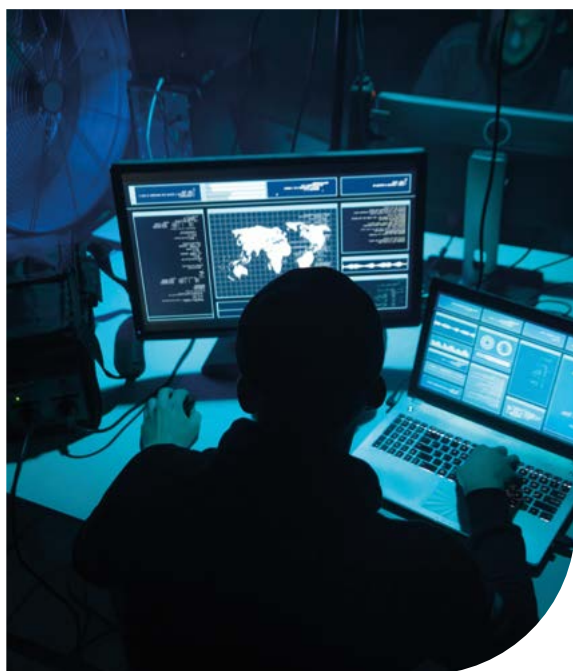


adw. Przemysław Barchan
Instytut LegalTech NRA, ELTA

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 kancelarii prawnych.

Średnia tygodniowa liczba cyberataków na świecie w połowie 2022 r. na przeciętną organizację wyniosła prawie 1200 razy (przy około 940 razach w Polsce). Zauważalny jest przy tym stały wzrost liczby ataków. Z uwagi na sytuację geopolityczną naszego regionu i trwający konflikt zbrojny statystyki te wzrosły w Polsce do **ponad 1200 razy tygodniowo**.

Tegoroczna edycja Raportu LegalTech 2023 prezentuje ciekawe statystyki styczności kancelarii prawnych



w Polsce z cyberatakami. Zgodnie z tymi badaniami **33% ankietowanych kancelarii miało styczność z cyberatakami** (przy odpowiednio 26% w edycji na 2022 r. i 30% w edycji na 2021 r.). Choć dane te wydają się być zaniżone względem rzeczywistej liczby ataków i nie uwzględniają ich skuteczności, to pokazują tendencję wzrostową (zgodną z trendem światowym).

Spośród rodzajów cyberataków ankietowani wskazują głównie na *phishing* (57% ankietowanych), złośliwe oprogramowanie (*malware*, 33%) oraz ataki DoS (*Denial of Service*, 18%). Dane te prezentują **ogólną tendencję phishingu do dominowania wśród ataków** (szacuje się, że ok 3,4 mld wiadomości e-mail dziennie stanowi *phishing*).

Phishing stanowi największe bezpośrednie zagrożenie dla branży prawnej.

Atak ten bazuje na działaniach socjotechnicznych atakującego, odwołując się do emocji lub wprowadzając adresata w błąd w celu wyłudzenia określonego działania (głównie udzielenia dostępu lub w celu kradzieży środków finansowych). Służy też jako pierwsza forma ataku przed atakiem docelowym (np. *malware* lub *ransomware*). *Phishing* dzielimy na: *spear-phishing* (atak nakierowany na konkretną grupę lub osoby), *whaling* (tzw. atak na „grubą rybę”, np. partnera zarządzającego kancelarią), *smishing* (atak przy wykorzystaniu sms-ów z linkami lub komunikatorów) oraz *angler phishing* (atak przy wykorzystaniu social mediów z linkami lub w celu wyłudzenia danych profilowych). Ogólnodostępne statystyki sugerują, że w przypadku dwóch ostatnich form ataku *phishingowego* najpopularniejszymi narzędziami wykorzystywanymi do ataku jest LinkedIn i WhatsApp. *Phishing* stanowi **największe bezpośrednie zagrożenie dla branży prawnej**, która jest znacznie mniej zabezpieczona przed cyberatakami niż znaczna część

CYBERZAGROŻENIA w pracy prawnika

klientów kancelarii. Z perspektywy atakującego zdecydowanie prostszym i bardziej skutecznym działaniem jest podjęcie próby uzyskania dostępu do danych klienta kancelarii poprzez *spear-phishing* lub *whaling* skierowane na personel kancelarii (w formie tzw. *consent phishing*) niż podejmowanie próby ataku na infrastrukturę klienta kancelarii.

Mając to na uwadze, cyberbezpieczeństwo powinno stanowić krytyczne pole zainteresowania branży prawnej. Dostrzegła to m.in. Naczelna Rada Adwokacka, która przyjęła w styczniu 2023 r. **Dobre praktyki dotyczące cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata** przygotowane przez Instytut LegalTech przy Naczelnej Radzie Adwokackiej.

Widząc powyższe zagrożenia, kancelarie i prawnicy dostrzegają potrzebę właściwego zabezpieczenia się przed cyberatakami. Zgodnie z danymi przedstawionymi w *Raporcie LegalTech 2023* do najpopularniejszych

Średnia tygodniowa liczba cyberataków w Polsce na przeciętną organizację wzrosła do ponad 1200 razy tygodniowo.

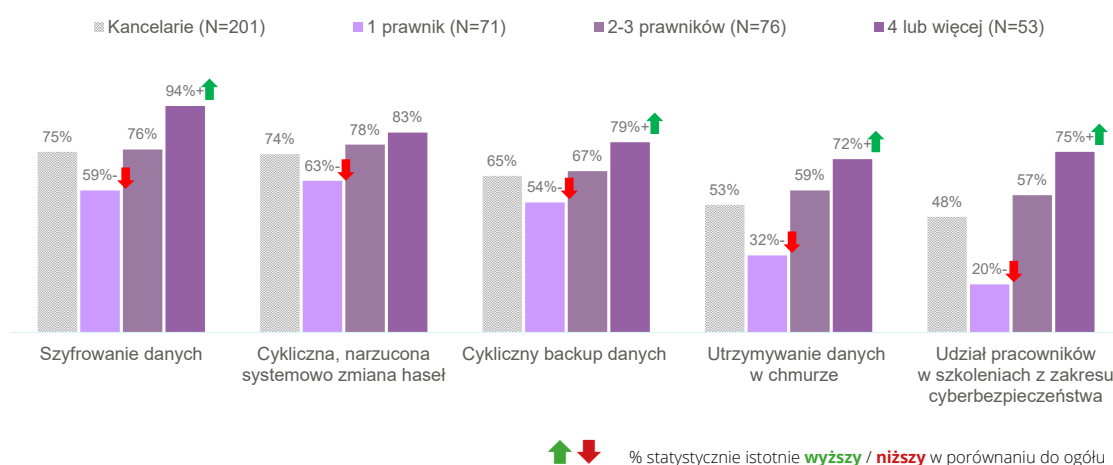
zabezpieczeń stosowanych przez kancelarie należą: szyfrowanie danych (75% ankietowanych), cykliczna zmiana haseł (74%) oraz cykliczny back-up danych (65%). Badanie pokazuje również, że skala stosowania zabezpieczeń zależy w głównej mierze od wielkości kancelarii, tj. im większa kancelaria, tym większe prawdopodobieństwo stosowania określonych zabezpieczeń. Zaprezentowany w badaniu poziom procentowy udziału w szkoleniach z zakresu cyberbezpieczeństwa nie jest optymistyczny, biorąc pod uwagę, że statystycznie najwięcej kancelarii w Polsce jest 1-, 2-, 3-osobowych.

Zadaniem samorządów zawodowych powinno być więc popularyzowanie zagadnień związanych z tą tematyką w celu podniesienia świadomości w tym zakresie.

SPOSOBY ZABEZPIECZENIA kancelarii przed cyberatakiem

Do najpopularniejszych zabezpieczeń stosowanych przez kancelarie należą: szyfrowanie danych (75%), cykliczna zmiana haseł (74%) oraz cykliczny back up danych (65%).

Różnego rodzaju zabezpieczenia technologiczne przed cyberatakiem istotnie częściej stosowane są przez większe kancelarie, zatrudniające 4 lub więcej pracowników.



Podstawa: Kancelarie: N=201

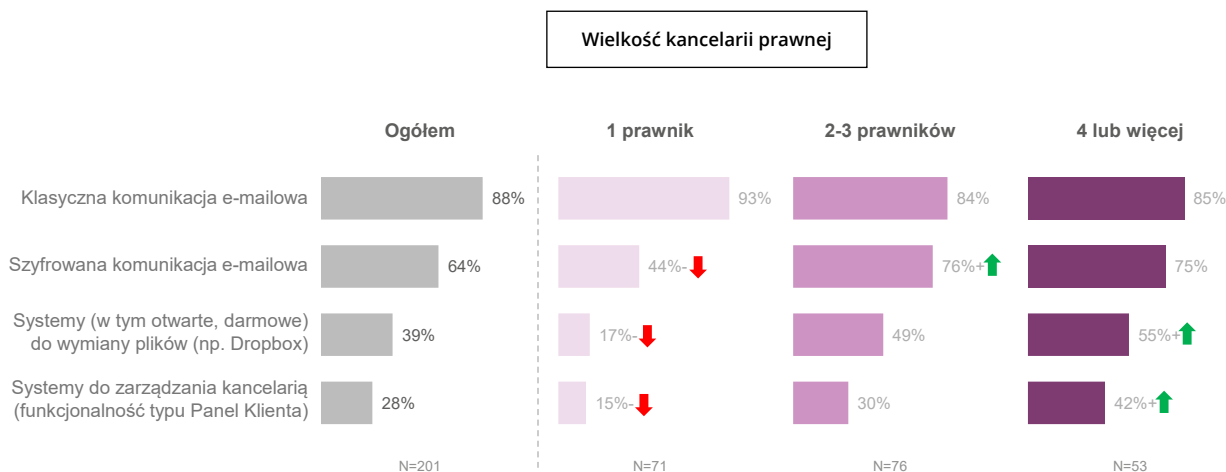
Wykres 14. W jaki sposób Pana(i) kancelaria jest zabezpieczana technologicznie? Proszę o wskazanie rozwiązań, które są stosowane w Pana(i) miejscu pracy.

KOMUNIKACJA kancelarii z klientami

Zdecydowanie najczęstszym sposobem komunikacji kancelarii z klientem nadal pozostaje klasyczna komunikacja mailowa (**88%**).

Z szyfrowanej komunikacji e-mail korzysta **64%** badanych kancelarii; istotnie rzadziej praktyka ta dotyczy najmniejszych kancelarii (**44%**).

Mniej popularne sposoby komunikowania się z klientami, np. za pomocą systemów do wymiany plików, takich jak Dropbox czy systemów do zarządzania kancelarią, istotnie częściej praktykowane są w większych kancelariach.



Podstawa: Kancelarie; N=201

Wykres 15. W jaki sposób Pana(i) kancelaria komunikuje się z Klientami – wysyła i odbiera poufną korespondencję, dokumenty?

↑ ↓ % statystycznie istotnie **wyższy** / **niższy** w porównaniu do ogółu



r. pr. Artur Piechocki
APLaw

Badania wykonane przez Kantar i C.H.Beck wskazują na wyraźne statystyczne umacnianie się pozycji podstawowych form zagrożeń dla bezpieczeństwa systemów informatycznych stosowanych przez kancelarie prawne. Dominuje **phishing**, jako najprostsza, najtańsza i najbardziej efektywna forma ataku. Wykorzystanie przez przestępców naiwności, niefrasobliwości czy po prostu chwili nieuwagi ofiary zapewnia szybki sukces. Wystarczy kliknięcie w link, który z pozoru pochodzi od znanego nam klienta kancelarii albo firmy kurierskiej i otwiera się droga do zasobów komputera i systemu informacyjnego. W dalszej kolejności pojawia się **oprogramowanie złośliwe**, które wykrada hasła, wprowadza ransomware itp.

Niektóre z zagrożeń podawanych przez respondentów jako najczęściej pojawiające się w kancelariach mogą pokrywać się phishingiem, dlatego faktyczna liczba ataków typu phishing może być nawet wyższa niż wskazana w statystykach. Użycie oprogramowania złośliwego może być po prostu następstwem zastosowania inżynierii społecznej, dokonanie działania określanego jako **hacking wetware**, czyli wykorzystania do przeprowadzenia ataku samej osoby, która jest jego celem.

Pamiętajmy, że zamiarem przestępców jest zwykle uzyskanie dostępu do naszych pieniędzy, dlatego próby muszą być podejmowane na masową skalę, im jest ich więcej, tym większe prawdopodobieństwo sukcesu. Takie działanie wymaga z kolei niskich kosztów. Phishing,

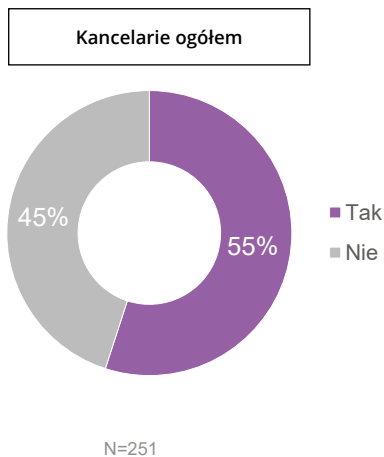
w którym sama ofiara „pomaga” przestępcy, jest wyjątkowo korzystny pod tym względem, jest po prostu bardzo tanią formą ataku, niewymagającą szczególnych nakładów finansowych.

Wśród zjawisk wymienionych w raporcie warto wskazać na **niższy poziom ataków typu ransomware**. Być może jest to wynik skuteczniejszej ochrony zasobów posiadanych przez kancelarie. Ochrona taka realizowana jest przez częstsze wykonywanie kopii zapasowych, backupów oraz korzystania z chmury obliczeniowej.

Wśród mniejszych kancelarii stopień zabezpieczenia przed zagrożeniami internetowymi jest znacznie niższy niż w większych podmiotach, co jest zrozumiałe ze względu na rosnące koszty rozwiązań informatycznych z zakresu cyberbezpieczeństwa. Z drugiej jednak strony nic nie usprawiedliwia braku stosowania elementarnych zasad prewencji, jak np. nieczęsty udział w szkoleniach, które bardzo często mają charakter nieodpłatny.

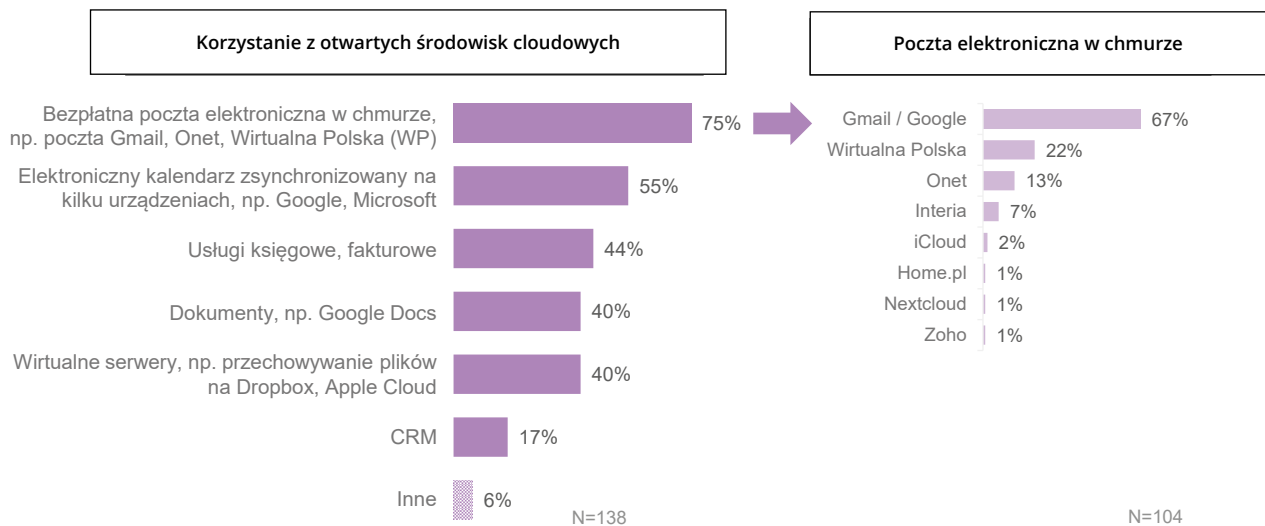
Generalnie należy ocenić bardzo pozytywnie tendencje zwykłe obserwowane w raporcie. Szczególnie cieszą **wzrosty w korzystaniu z chmury, stosowanie szyfrowania i backupu danych**. Nie zapominajmy, że powierzenie zarządzania naszymi zasobami profesjonalistom minimalizuje nasze ryzyko, a tym samym lepiej chronimy dane naszych Klientów.

Korzystanie z otwartych środowisk CLOUDOWYCH



Z otwartych środowisk cloudowych korzysta w swojej pracy coraz więcej prawników; w obecnym pomiarze korzystanie z takich rozwiązań zadeklarowało **55%** z nich (w 2022 – **48%**).

Nadal najpopularniejsza jest bezpłatna poczta elektroniczna w chmurze (**75%**), stosunkowo często prawnicy korzystają również z elektronicznego kalendarza zsynchronizowanego na kilku urządzeniach (**55%**).



Podstawa: wszyscy respondenci; N=251

Wykres 16. Czy korzysta Pan(i) w swojej pracy zawodowej z otwartych środowisk cloudowych, jak np. Dropbox, Google docs, poczta elektroniczna w chmurze, np. Gmail?

Wykres 17. Z jakich konkretnie rozwiązań Pan(i) korzysta? Czy jest to...

Wykres 18. Z usług konkretnie którego dostawcy poczty elektronicznej w chmurze Pan(i) korzysta w celu świadczenia usług prawniczych?



ZŁOŚLIWE OPROGRAMOWANIA i *phishing* zagrażają kancelariom



dr hab. inż. prof. ucz.
Agnieszka Gryszczyńska
UKSW, Prokuratura Krajowa

Cyberprzestępczość jest jedną z najbardziej dynamicznych form przestępczości. **Sprawców cyberprzestępstw cechuje wysoki poziom adaptacyjności** – dla osiągnięcia założonego celu szybko dostosowują zarówno metody, wykorzystywane narzędzia, jak również socjotechnikę związaną z atakami.

W Polsce obserwuje się zarówno ataki o globalnym, jak i lokalnym charakterze. Oprócz *aktorów* globalnych – zajmujących się dystrybucją złośliwego oprogramowania, dezinformacją, atakami wymierzonymi w poufność danych czy w łańcuchy dostaw, istotnym zagrożeniem jest również działalność polskich cyberprzestępców nakierowanych głównie na korzyści majątkowe.

Sprawcy korzystają z nowoczesnych rozwiązań technologicznych pozwalających na zachowanie anonimowości, sprawną komunikację oraz transfer środków pochodzących z przestępczego procederu. W celu ukrycia własnej tożsamości kreują nową tożsamość lub wykorzystują dane innych osób. Przestępstwa popełnienie są przez nich indywidualnie, jak też w ramach wysoko wyspecjalizowanych i zorganizowanych grup przestępczych. Podkreślenia wymaga, że aktualnie sprawcy nie muszą mieć specjalistycznej wiedzy czy zaawansowanych umiejętności z uwagi na to, że wykorzystanie modelu usługowego Cybercrime-as-a-Service znacząco obniża tzw. „barierę wejścia” dla mniej technicznych osób.

Analiza raportów dotyczących cyberbezpieczeństwa wskazuje na stały, znaczny wzrost liczby incydentów zarówno w Polsce, jak i na świecie. **Zdalna praca, edukacja czy realizacja zadań publicznych online, wymuszone podczas pandemii, stały się dla cyberprzestępców okazją do zwiększenia skuteczności ataków** zarówno na duże korporacje, małych przedsiębiorców, administrację publiczną, szpitale, jak i osoby fizyczne. W 2020 i 2021 r. dominowały więc scenariusze związane z pandemią. W związku z atakiem Federacji Rosyjskiej na Republikę Ukrainy w 2022 r. obserwowane są zarówno **ataki o hybrydowym charakterze, jak**

również wykorzystywane w scenariuszach socjotechnicznych wojny.

Jak wynika z przygotowanego *Raportu LegalTech 2023* dotyczącego cyberzagrożeń w pracy prawnika, **z próbami cyberataków spotkało się 33% kancelarii**, co stanowi wzrost o 7% w porównaniu z badaniem przeprowadzonym w 2022 roku.

Najczęstszymi kategoriami incydentów były *phishing* (57%), złośliwe oprogramowanie (33%), ataki odmowy usługi (18%) oraz ataki *ransomware* (3%).

Kategorie zagrożeń nie zmieniły się zatem znacząco w porównaniu z ubiegłym rokiem, jednak zauważalny jest wzrost ataków odmowy usługi (DDoS). Ekspert z zakresu cyberbezpieczeństwa wskazuje, że ataki DDoS **mają podłoże geopolityczne i są jednym z instrumentów wykorzystywanych w ramach wojny w Ukrainie.** Ich celem są nie tylko strony konfliktu, ale również kraje udzielające wsparcia Ukrainie, w tym w szczególności Polska. Atakom DDoS sprzyja nie tylko rozwój botnetów, a również dostępność usług w modelu DDoS-as-a-Service.

Dane z badań dotyczących kancelarii można zestawić także z danymi dotyczącymi incydentów publikowanymi przez zespół CSIRT GOV oraz CERT Polska, z tym jednak zastrzeżeniem, że nie zostały jeszcze opublikowane raporty dotyczące 2022 roku. Analiza raportów CERT Polska wskazuje, że zdecydowanie dominuje *phishing*, którego udział na tle innych typów incydentów stale i znacząco rośnie. W 2021 r. *phishing* stanowił aż 77 % wszystkich obsługiwanych incydentów.

Najpopularniejszym atakiem phishingowym w 2021 r. było podszywanie się pod serwis społecznościowy Facebook. Do wyłudzenia danych najczęściej dochodziło poprzez stronę imitującą panel logowania do zaufanej usługi (poczty elektronicznej, serwisu

CYBERZAGROŻENIA w pracy prawnika

społecznościowego czy bankowości elektronicznej). Linki do stron wyłudających dane do logowania do różnych usług wysyłane są zarówno pocztą elektroniczną, jak również w wiadomości SMS (*smishing*). W ostatnich latach coraz częściej do wyłudzenia danych dochodzi w trakcie rozmowy telefonicznej (*vishing*), podczas której sprawcy podszywają się pod numer telefonu zaufanego podmiotu (tzw. *CallerID spoofing*).

Podszywanie się pod inne podmioty ma służyć przede wszystkim zwiększeniu skuteczności ataku. Wiadomości mają sprawiać pozory autentyczności, dlatego najczęściej sprawcy wykorzystują spoofing adresów e-mail lub numerów telefonów lub wysyłają wiadomości z adresów poczty elektronicznej lub podobnych do adresów podmiotów, pod które się podszywają.

Sprawcy tworzą konta poczty elektronicznej u popularnych dostawców usług elektronicznych, wykorzystując tożsamość konkretnych osób lub tworzą konta poczty elektronicznej po wcześniejszym zarejestrowaniu nazwy domenowej podobnej do nazwy domenowej podmiotu, pod który się podszywają.

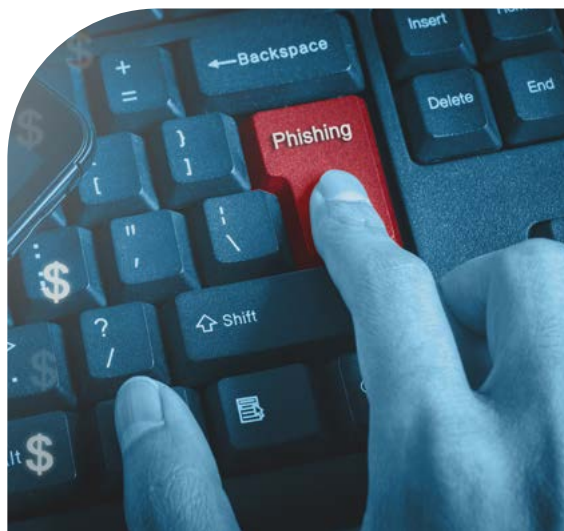
W opublikowanym 7 marca 2023 roku raporcie pt. „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości” Najwyższa Izba Kontroli oceniła jako nierzetelne i nieskuteczne działania mające na celu edukowanie i ostrzeganie obywateli na temat niebezpieczeństw grozących im ze strony sprawców przestępstw internetowych, w tym kradzieży tożsamości. Zastrzeżenia dotyczyły również nierzetelnego przygotowania oraz braku należytej koordynacji strategicznych dokumentów wyznaczających cele i priorytety państwa w obszarze cyberbezpieczeństwa, tj. „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024” oraz „Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa”. Kontrola pozwoliła również zidentyfikować szereg barier, które utrudniają obywatelom uzyskanie skutecznego wsparcia w sytuacji pokrzywdzenia przestępstwem. NIK ocenił jednocześnie pozytywnie utworzenie w 2022 r. nowej jednostki organizacyjnej Policji wyspecjalizowanej w zwalczaniu przestępczości internetowej – Centralnego Biura Zwalczania Cyberprzestępczości.

Analiza raportów CERT Polska wskazuje, że zdecydowanie dominuje **phishing**, którego udział na tle innych typów incydentów stale i znacząco rośnie.

W zakresie ograniczania skutków kradzieży tożsamości oraz przeciwdziałania *smishingowi*, *vishingowi* i *spoofingowi* podjęto jednak w ostatnim roku prace legislacyjne. Na etapie rządowego procesu legislacyjnego pozostają prace nad ustawą o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości (projekt z 12 grudnia 2022 r.), której istotą jest umożliwienie osobie, której dane dotyczą, zastrzeżenia numeru PESEL. 2 marca 2023 r. do Sejmu wpłynął rządowy projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (druk nr 3069), który wprowadzić ma nie tylko nowe typy czynów zabronionych i sankcje karne za wysyłanie wiadomości, w których podszyto się pod inny podmiot, ale również regulację o charakterze administracyjnym odnoszącą się do blokowania krótkich wiadomości tekstowych (SMS) zawierających treści zawarte we wzorcu wiadomości uznanej za nadużycie.

Zgodnie z projektem, **wprowadzony ma zostać otwarty katalog nadużyć w komunikacji elektronicznej**, przy czym w projekcie dookreślono cztery podstawowe formy nadużyć w komunikacji elektronicznej, którymi są:

- **generowanie sztucznego ruchu** – wysyłanie lub odbieranie komunikatów lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe;



CYBERZAGROŻENIA w pracy prawnika

- **smishing** – wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania;
- **CLI spoofing** – nieuprawnione posłużenie się lub korzystanie przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służące podszyciu się pod inny podmiot w szczególności w celu wywołania strachu lub poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego działania, zwłaszcza przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania;
- **nieuprawniona zmiana informacji adresowej** – nieuprawnione modyfikowanie informacji o numerze lub identyfikatorze użytkownika wysyłającego komunikat (identyfikatorem mogą być np. adresy elektroniczne, nazwy, kody czy adresy IP) uniemożliwiające lub istotnie utrudniające ustalenie, przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu numeru telefonu lub identyfikatora, przy użyciu którego nastąpiło wysłanie komunikatu elektronicznego.

Dla kształtowania cyberbezpieczeństwa i budowania odporności na cyberataki konieczne są zróżnicowane działania. Dla zwiększenia odporności na najczęściej występujące w kancelariach ataki phishingowe **należy**

pamiętać o weryfikowaniu danych (np. sprawdzenia poprawności adresu strony internetowej logowania), stosowaniu uwierzytelnienia dwuskładnikowego (najlepiej opartego o klucz do dwuetapowego uwierzytelnienia U2F) oraz stałym szkoleniu pracowników.

Niestety przed atakami phishingowymi nie chronią najpopularniejsze, wskazane w raporcie zabezpieczenia stosowane przez kancelarie – w szczególności nie chroni przed nimi cykliczna zmiana haseł (wskazana przez 74% kancelarii).

Połączenie klucza do dwuetapowego uwierzytelnienia wraz z podnoszeniem cyberhigieny i cyberodporności zatrudnionych w kancelariach prawniczych **może wymiernie ograniczyć skuteczność cyberataków.**

Cieszyć powinien wskazany w raporcie wzrost udziału pracowników kancelarii w szkoleniach z zakresu cyberbezpieczeństwa, jednak nadal wynosi on poniżej 50%. Co więcej, widoczny jest spadek w tym zakresie w segmencie kancelarii jednoosobowych.

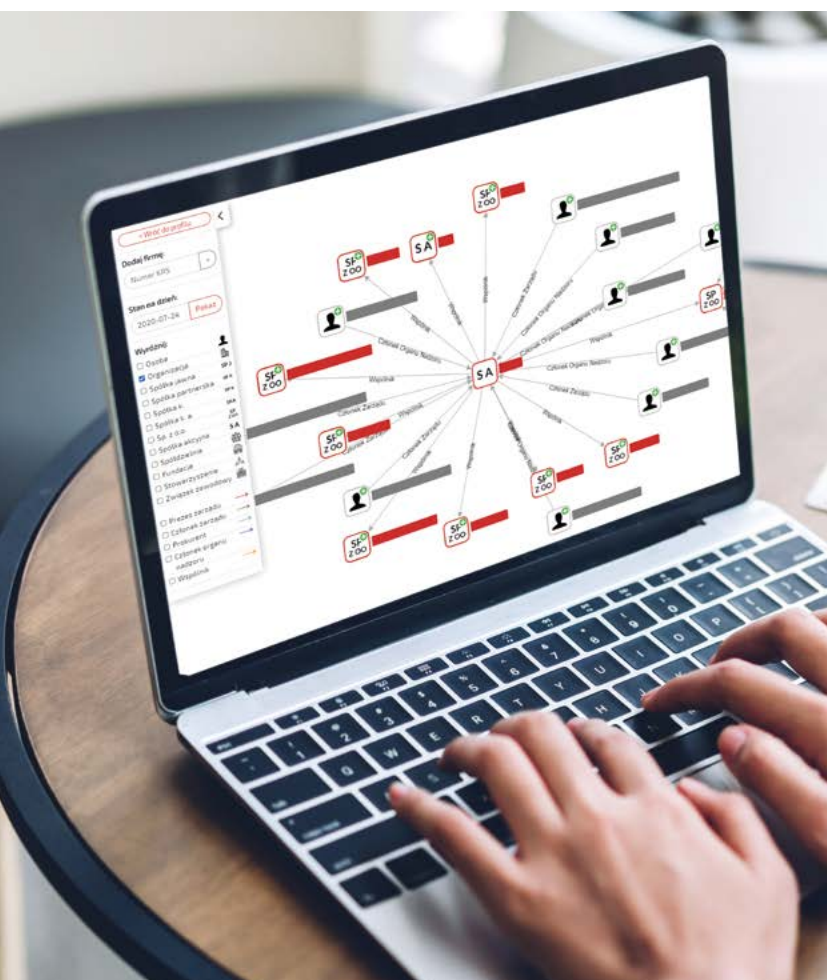
W tym miejscu warto wspomnieć o działaniach, które dla segmentu małych i średnich przedsiębiorstw przygotował NASK. 8 marca 2023 r. podczas spotkania inauguracyjnego „Program edukacji i certyfikacji cyberbezpieczeństwa dla biznesu” złożono deklarację praktycznego wsparcia przedsiębiorców we wdrażaniu sprawdzonych, najlepszych praktyk i zasad ochrony w środowisku cyfrowym oraz podnoszenia kompetencji w tym obszarze. Uruchomiono również możliwość zapisania się do pilotażu programu certyfikacji.



beck **KRS**

Informacja Gospodarcza

Bezpieczeństwo
obrotu
gospodarczego



- Połączone źródła danych z **Krajowego Rejestru Sądowego** oraz **Monitora Sądowego i Gospodarczego**.
- Ocena **standingu finansowego** przedsiębiorstwa w oparciu o sprawozdania finansowe z e-KRS.
- Dodatkowe źródła danych o podmiocie: **dofinansowania, zamówienia publiczne, zadłużenia**.
- **Graficzne powiązania biznesowe** z osobami i podmiotami.

Wejdź na **konfigurator.legalis.pl**

Kup online - korzystaj od razu!



SZTUCZNA INTELIGENCJA a zawód prawnika

ZADANIA PRAWNIKA, których
nie zastąpi sztuczna inteligencja

Korzystanie z narzędzi
wykorzystujących
SZTUCZNĄ INTELIGENCJĘ

Jakie aspekty pracy prawnika są poza zasięgiem **SZTUCZNEJ INTELIGENCJI**?



r. pr. dr Aleksandra Auleytner
Domański Zakrzewski Palinka

Przeprowadzone przez C.H.Beck w 2023 r. wśród różnych profesji prawniczych badanie pokazało, że zdaniem respondentów sztuczna inteligencja na pewno nie zastąpi pracy prawnika w przypadku niestandardowych spraw (56%). Dodatkowo ok. 50% badanych wskazywało na obszar kontaktu z klientem, jako ten, który nie może być zastąpiony przez sztuczną inteligencję.

Wnioski z tego badania są szczególnie ciekawe wśród rosnącego zapotrzebowania na wsparcie pracy prawniczej przez **różnego rodzaju narzędzia wspomagane przez AI**. Są też interesujące w kontekście pojawiających się z dużą intensywnością coraz większej liczby nowych rozwiązań informatycznych opartych o tzw. Generative AI – jak np. Chat GPT – idących jeszcze dalej niż dotychczas znane narzędzia analityczne. Generują one bowiem nowe treści – odpowiedzi na pytania, notatki, treści e-maili, opracowania w bardzo krótkim czasie. Jakkolwiek narzędzia te są jeszcze ułomne, a np. **odpowiedzi Chatu GPT często opatrzone są błędami, rażącymi powtórzeniami i informacjami nieakceptowalnymi w profesjonalnej pracy prawniczej**, nie sposób wykluczyć, że w przyszłości zostaną one udoskonalone.

Wyniki badania zleconego przez C.H.Beck pokazują w zasadzie, które **elementy profesji prawniczej są unikalne i niezastępowalne**. Wskazują więc też, które elementy naszej codziennej aktywności prawniczej wymagają największej uwagi i ciągłego doskonalenia. Tym obszarem są zadania, które wymagają empatii, kreatywności i wiedzy praktycznej, a także zdolności rozwiązywania niestandardowych problemów. Na pierwszy plan wybija się tu obszar **relacji pomiędzy klientem a prawnikiem**. Relacja ta wymaga zaufa-

nia, akceptacji i zdolności interpersonalnych dających możliwość zapewnienia klientowi właściwego poczucia bezpieczeństwa w prowadzonych dla niego sprawach. **Obszar relacji klient – prawnik wymaga więc intuicji, zdolności komunikacyjnych oraz praktycznego doświadczenia**, a więc umiejętności, które nie są dostępne dla sztucznej inteligencji. Umiejętności te są szczególnie ważne w trakcie doradztwa prawnego przy negocjacjach czy rozwiązywaniu sytuacji konfliktowych, z którymi klient styka się w codziennej, biznesowej aktywności.

Przy okazji sama zadałam pytanie Chatowi GPT na temat tego, **w jakich zadaniach sztuczna inteligencja nie zastąpi człowieka**. Chat GPT, oprócz obszernej analizy na temat braku zdolności interpersonalnych sztucznej inteligencji, dał taką odpowiedź:

- 1. Rozumienie kontekstu społecznego i kulturowego** – sztuczna inteligencja może dostarczyć dużo danych i analiz, ale nie ma wiedzy na temat konkretnych kwestii społecznych i kulturowych, które mogą wpłynąć na decyzje prawnika.
- 2. Ocena dowodów** – ocena dowodów wymaga ludzkiej intuicji, zdolności do zrozumienia kontekstu i interpretacji niuansów, które mogą mieć znaczenie w sprawie.

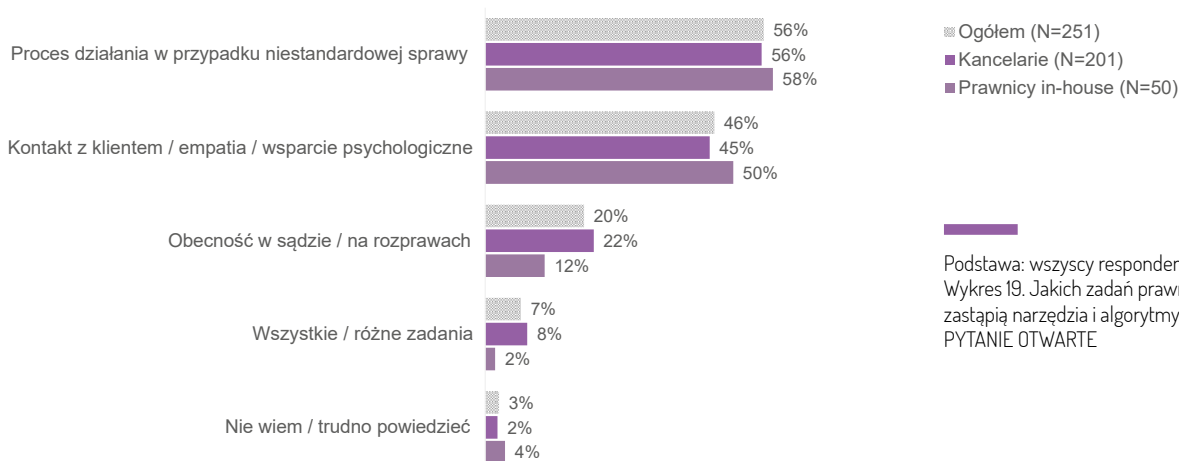
Wydaje się więc, że **sztuczna inteligencja nie szybko będzie w stanie rozwiązać problemy, które wymagają niestandardowego, twórczego myślenia lub stworzenia wysokiej jakości relacji interpersonalnych opartych na zaufaniu i zrozumieniu**. Właśnie w takim m.in. zakresie zadania te będą zawsze zarezerwowane dla prawników.

ZADANIA PRAWNIKA, których nie zastąpi sztuczna inteligencja

Najczęściej, badani prawnicy byli zdania, iż sztuczna inteligencja nie zastąpi pracy prawnika w przypadku niestandardowych spraw (56%).

Blisko 50% wskazywało na obszar kontaktu z klientem, jako niemożący być zastąpiony przez sztuczną inteligencję.

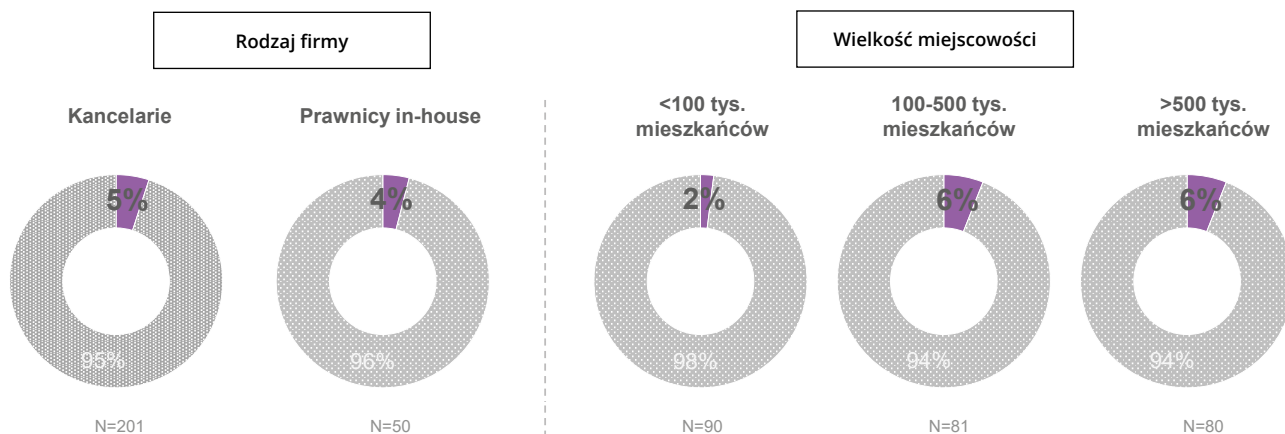
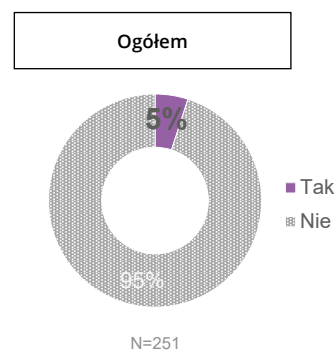
Co piąty badany podnosił kwestię osobistej obecności prawnika w sądzie, na rozprawach.



Podstawa: wszyscy respondenci; N=251
Wykres 19. Jakich zadań prawnika nie zastąpią narzędzia i algorytmy?
PYTANIE OTWARTE

Korzystanie z narzędzi wykorzystujących SZTUCZNĄ INTELIGENCJĘ

Korzystanie w pracy prawniczej z narzędzi wykorzystujących sztuczną inteligencję jest niewielkie i dotyczy około 5% prawników. Nieco częściej narzędzi takich używają prawnicy z większych ośrodków miejskich.



Podstawa: wszyscy respondenci; N=250
Wykres 20. Czy korzysta Pan(i) lub zetknął(ęła) się w pracy prawniczej z narzędziami wykorzystującymi sztuczną inteligencję?

WYKORZYSTANIE AI do poszerzania zakresu i poprawy jakości usług prawniczych



r. pr. dr Gabriela Bar
Szostek_Bar i Partnerzy

Konkluzje raportu odzwierciedlają powszechne w branży prawniczej przekonania co do możliwości AI. Moim zdaniem jednak **jest tylko kwestią czasu to, żeby AI zastąpiła prawników w zdecydowanej większości zadań**, które wykonują.

Sądzę, że prawnicy powinni bardziej skupić się na **wykorzystaniu AI do poszerzania zakresu swoich usług i poprawy ich jakości**, a nie na obawach, że zostaną przez nią zastąpieni. W nieodległej przyszłości partnerzy kancelarii lub szefowie działów prawnych mogą mieć unikalną (w dotychczasowej historii) możliwość zarządzania multidyscyplinarnymi zespołami, w których AI będzie jednym z ważnych elementów lub nawet – członkiem zespołu.

Tak zwane centaury AI mogą stanowić dynamiczną i bardzo efektywną strukturę, w której ludzie mają do odegrania ważną rolę dzięki swoim unikalnym cechom i zdolnościom: intelektualnemu osądowi, empatii, kreatywności i zdolnościom adaptacyjnym. Rzeczywiście bowiem nawiązywanie i utrzymywanie relacji z klientem to obszar, który prawdopodobnie najdłużej będzie domeną prawników-ludzi.

...prawnicy powinni bardziej skupić się na wykorzystaniu AI do poszerzania zakresu swoich usług i poprawy ich jakości, a nie na obawach, że zostaną przez nią zastąpieni...

Nieco zaskakujący jest wynik 5% w odniesieniu do wykorzystania przez prawników w ich pracy narzędzi opartych na AI. Być może prawnicy nie zdają sobie sprawy z tego, że algorytmy AI znajdziemy w wielu systemach IT, np. popularnym Office365 czy też w wyszukiwarkach internetowych Google lub Microsoft.

Niektóre systemy informacji prawnej, z których korzystają chyba wszyscy prawnicy, także mają funkcje oparte na AI.

Prawdopodobnie wciąż za mało jest szkoleń w zakresie innowacji technologicznych, które prawnicy mogliby stosować w codziennej pracy. Wiele izb radcowskich i adwokackich w Polsce stara się to zmienić, organizując wykłady i warsztaty na ten temat.



adw. Xawery Konarski
Traple, Konarski,
Podrecki i Wspólnicy

*Legal tech stał się istotną częścią działalności prawników. Cieszy, że dostrzegają to samorzędy zawodowe, w szczególności Naczelna Rada Adwokacka i Krajowa Izba Radców Prawnych. Mają one do odegrania bardzo ważną rolę na trzech płaszczyznach. Po pierwsze, w zakresie **edukacji** odnośnie do doboru odpowiednich narzędzi teleinformatycznych wspierających prace adwokatów i radców prawnych. Po drugie, poprzez przyjmowanie **dobrych praktyk** określających, jak z tych narzędzi korzystać (np. wymogi dotyczące cyberbezpieczeństwa). Po trzecie, w drodze odpowiednich zmian **kodeksów etyki i godności zawodu**, uwzględniających ryzyka wykonywania zawodu prawnika w środowisku cyfrowym.*

Jako Stowarzyszenie Prawa Nowych Technologii postulujemy, aby powyższe działania prowadziły do wypracowania przez samorzędy prawnicze wspólnych standardów. Często bowiem adwokaci i radcowie prawni wykonują działalność w ramach jednej kancelarii prawnej, a stosowanie się do różnych wymogów korporacyjnych, np. w zakresie korzystania z poczty elektronicznej, jest dużym i niepotrzebnym utrudnieniem organizacyjnym.

Środowisko prawnicze w Polsce jeszcze **NIE ZAREAGOWAŁO NA REWOLUCJĘ AI**



prof. Grzegorz Sibiga
Traple, Konarski, Podrecki
i Wspólnicy
Instytut Nauk Prawnych PAN

Wyniki badania pokazują, że **środowisko prawnicze w naszym kraju jeszcze nie zareagowało na rewolucję AI**, która, jak się wydaje, właśnie rozpoczęła się na naszych oczach. Dotychczasowa skala wykorzystania przez kancelarie rozwiązań dla nich dedykowanych nie była imponująca i to mimo całkiem bogatej oferty, co potwierdza *Raport LegalTech 2023*.

Natomiast niespotykany dotychczas w innych rozwiązaniach wzrost liczby użytkowników ChatGPT – pierwszego tak powszechnie dostępnego narzędzia, uwidacznia, jakie mogą nastąpić zmiany w wykonywaniu niektórych zawodów opartych na pracy umysłowej. Rewolucja polega bowiem również na tym, że ChatGPT unaocznia nam jak nigdy dotąd, że łatwo dostępne narzędzia mogą służyć nie tylko wsparciu pracy

(np. poprzez analizę danych czy automatyzację tworzenia dokumentów), ale prowadzić do pełnego zastąpienia pracy umysłowej człowieka, chociaż technologicznie nie stanowi to nowości.

Trzeba podkreślić, że chodzi o zastąpienie nie tylko w prostych, rutynowych czynnościach prawnych czy biurowych, ale także w tych skomplikowanych, wymagających wieloaspektowej analizy. Jednocześnie zawody prawnicze pojawią się w większości przygotowywanych przez ekspertów list zawodów, które mogą zostać zastąpione przez AI i to już w nie-dalekiej przyszłości.

Wydaje się, że już **nieuchronnie staje się w przyszłości zastąpienie udziału człowieka przynajmniej w części czynności prawniczych**, przy czym chodzi o zastąpienie faktyczne, a nie formalne.

Pozostają kluczowe pytania: w jakim zakresie oraz na jakich zasadach to nastąpi i wreszcie – jaka będzie rola prawnika-człowieka w tej nowej rzeczywistości. Stosowanie rozwiązań takich jak ChatGPT niesie bowiem ze sobą całą paletę problemów prawnych i etycznych. W szczególności dotyczą one **zachowania tajemnicy** (i przedsiębiorstwa, i zawodowej), zapewnienia warunków **ochrony danych osobowych**, przysługujących **praw autorskich**, czy **odpowiedzialności za rezultat działania** określonego narzędzia i **transparentności korzystania z AI** przez prawnika.

Niezależnie od wyników badań dotyczących aktualnego korzystania z AI, to już najwyższy czas, aby w tym zakresie nie tylko stawiać pytania, ale zacząć udzielać odpowiedzi.



beckakademia



Oferujemy
najwyższej jakości
wiedzę prawniczą



Najwyższy poziom
MERYTORYCZNY



Najlepsi
EKSPERCI



Aplikacja
MOBILNA



MATERIAŁY
szkoleniowe



Szeroki zakres
TEMATYCZNY



CERTYFIKAT
uczestnictwa

SZKOLENIA ZAMKNIĘTE

Organizujemy szkolenia zamknięte z zakresu prawa i podatków.
Nasi prelegenci to praktycy i eksperci w swoich dziedzinach.

Dopasujemy szkolenie do Twoich potrzeb i dostarczymy
najwyższej jakości wiedzę prawniczą.



FORMA SZKOLENIA:
STACJONARNIE
LUB ONLINE



INDYWIDUALNE
DOPASOWANIE



30 LAT
DOŚWIADCZENIA

Zapytaj o indywidualną ofertę szkolenia dla Twojego zespołu!

Napisz do nas: akademia@beck.pl lub zadzwoń: **22 311 22 22**

akademia.beck.pl

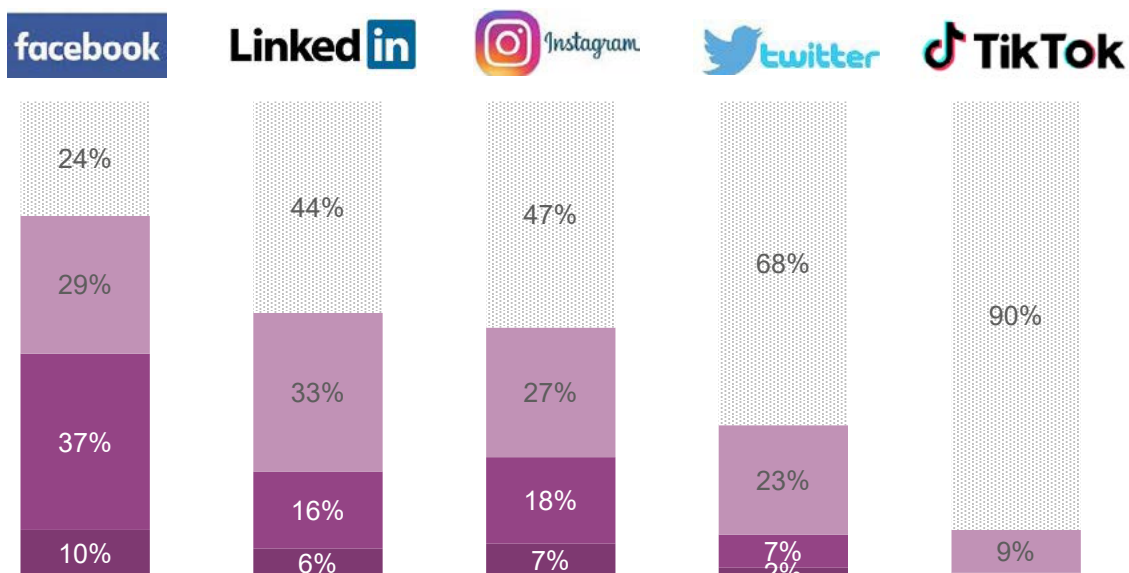
MEDIA SPOŁECZNOŚCIOWE



Korzystanie z serwisów społecznościowych

Wśród prawników najbardziej popularnym serwisem społecznościowym jest Facebook. Konto posiada tam **76%** badanych. Posiadanie kont na pozostałych serwisach jest na niższym poziomie – LinkedIn **55%**, Instagram **52%**, Twitter **32%** i TikTok – tylko **10%**.

W mediach społecznościowych częściej aktywni w są mecenasi z kancelarii zatrudniających 4 lub więcej prawników.



- Publikuję posty, komentuję
- Głównie śledzę wpisy i przeglądam informacje, zdjęcia
- Mam konto, ale rzadko tam zaglądam
- Nie posiadam konta w tym serwisie

Podstawa: wszyscy respondenci; N=251

Wykres 21. Jaki jest Pana(i) zwyczaj dotyczący korzystania z serwisu społecznościowego ...?

Metryczka – Charakterystyka zawodowa prawników kancelarii

Wykonywany zawód prawniczy



Podstawa: Kancelarie; N=201

Wykres 1. Proszę powiedzieć, jaki zawód Pan(i) wykonuje?

Wykres 2. Ilu prawników jest zatrudnionych w kancelarii, w której Pan(i) pracuje?

Liczba prawników zatrudnionych w kancelarii/dziale prawnym

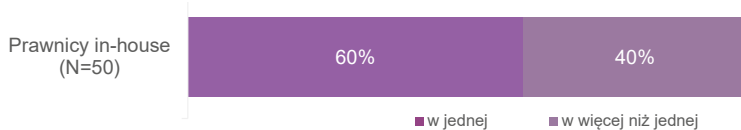


Podstawa: Prawnicy in-house; N=50

Wykres 3. Czy wykonując obowiązki prawnika w firmie, posiada Pan(i) uprawnienia...

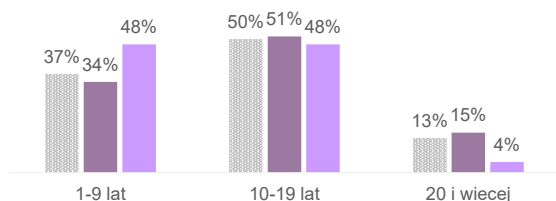
Wykres 4. Ilu prawników pracuje w dziale prawnym firmy, o której rozmawiamy?

Praca w jednej firmie czy w wielu?



Staż w zawodzie prawnika

■ Ogółem (N=251) ■ Kancelarie (N=201) ■ Prawnicy in-house (N=50)



Podstawa: Prawnicy in-house N=50 / wszyscy respondenci N=251

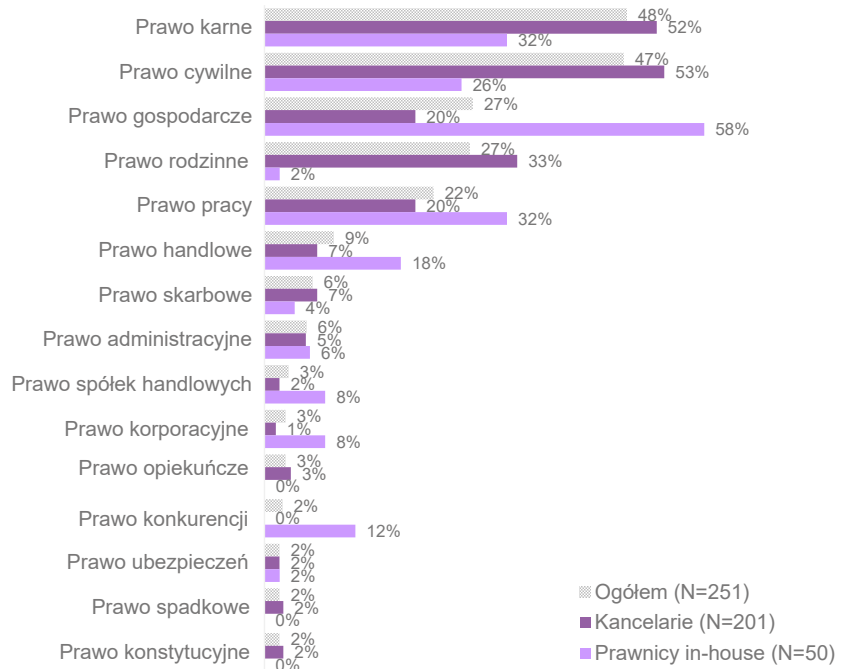
Wykres 5. Czy pracuje Pan(i) na stanowisku prawnika w więcej niż jednej firmie?

Wykres 6. Ile lat pracuje Pan(i) w zawodzie prawnika?

Metryczka – Charakterystyka zawodowa prawników kancelarii

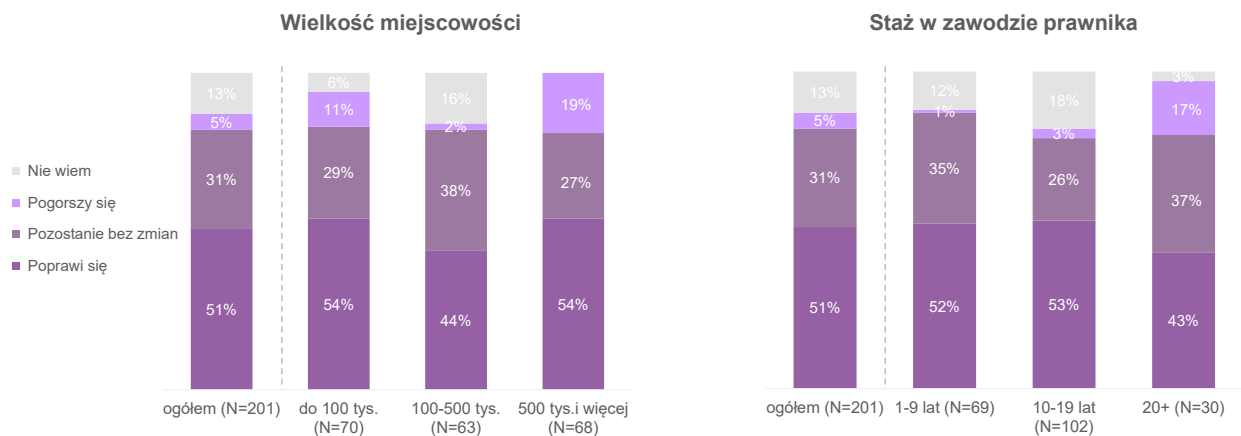
Obszary prawa, jakimi zajmują się badani prawnicy

(pokazane odpowiedzi >2% wskazań na poziomie ogółu)



Podstawa: Wszyscy respondenci; N=251
Wykres 7. Jakimi obszarami prawa się Pan(i) zajmuje?

Ocena sytuacji biznesowej kancelarii w perspektywie najbliższych dwóch lat



Podstawa: Kancelarie; N=201
Wykres 8. Czy, Pana(i) zdaniem, sytuacja biznesowa w Pana(i) kancelarii, w ciągu najbliższych dwóch lat...

PRAWO

NOWYCH TECHNOLOGII

Kompleksowe omówienie problematyki połączenia
prawa nowych technologii z pracą prawnika



ksiegarnia.beck.pl



KWARTALNIK

PRAWO NOWYCH TECHNOLOGII

PRAWO NOWYCH TECH

dane osobowe i prywatność / cyberbezpieczeństwo / handel elektroniczny

- DANE OSOBOWE I PRYWATNOŚĆ**
- ▶ Magdalena U. Miernik
Wizerunek a nowe technologie. Wizerunek
 - ▶ Artur Piechocki, Katarzyna Gorzkowska
Wybrane wyzwania dla ochrony prywatności
- INNOWACJE**
- ▶ Tomasz Świętnicki, Mateusz Jakubik
Nowe technologie w koncepcji inteligentnej
 - ▶ Dominik Sybilski
Nowe modele dzielenia się danymi w sprawie zarządzania danymi (DGA), i dostawcy usług pośrednictwa danych
- INTERNET I MEDIA**
- ▶ Charles Bouffier, Victoire Danès
A step towards legalising web scraping
 - ▶ Xawery Konarski
Unijny Akt o Usługach Cyfrowych - cel oraz najważniejsze obowiązki dostawcy
 - ▶ Magdalena Fiech
Wyłączenie odpowiedzialności dostawcy Aktu o Usługach Cyfrowych. Analiza



PRAWO NOWYCH TECHNOLOGII

www.czasopisma.beck.pl

NR 4/2022

dane osobowe i prywatność / cyberbezpieczeństwo / handel elektroniczny / innowacje / internet i media / prawo IT

- INNOWACJE**
- ▶ Damian Flisak
Metaversum: krótka charakterystyka rzeczywistości, która (może) nadejdzie
 - ▶ Katarzyna Grzybczyk
Metaverse - wiele hałasu o nic?
 - ▶ Aleksandra Auleytner, Marcin Jan Stepień
Źródła wirtualnych światów. Metaversum jako rezultat inspiracji, opracowania czy przejęcia?
 - ▶ Maciej Kubiak, Franciszek Dąbrowa
Metaversum a prawo autorskie - wybrane zagadnienia prawne
 - ▶ Anna Sokołowska-Ławniczak
Znaki towarowe w metaversie
 - ▶ Ewa Kurowska-Tober, Piotr Czulak
Metaverse a ochrona danych osobowych - problemy prawne, ryzyka i możliwe podejścia
 - ▶ Dominik Gabor
Prawo prywatne w metaversum
 - ▶ Katarzyna Staciwa
The Metaverse, Online Sexual Exploitation and Sexual Abuse of Children - a new challenge for today's global society?



C.H.BECK

C.H.BECK

Dane osobowe i prywatność
Cyberbezpieczeństwo
Handel elektroniczny
Innowacje ♦ Internet i media ♦ Prawo IT



ksiegarnia.beck.pl



ksiegarnia.beck.pl

Praktyczna Strona Prawa

Zamawiaj publikacje
na ksiegarnia.beck.pl



Wysyłka w 24h

Cenimy Twój czas.
Zamówienia realizujemy
nawet w 24 godziny.

Darmowa dostawa

Przy zakupie za min.
250 zł przesyłka
gratis.

Merytoryczne wsparcie

Odpowiadamy na pytania
i pomagamy wybrać
odpowiednie publikacje.

Odbiór osobisty

Odbierz zamówienie
w jednej z księgarni
C.H.Beck (Warszawa,
Wrocław, Poznań,
Katowice).

Newsletter

Dołącz do newslettera
i dowiedz się pierwszy
o nowościach
i promocjach.

Promocje

Sprawdź
aktualne oferty
na promocja.beck.pl

