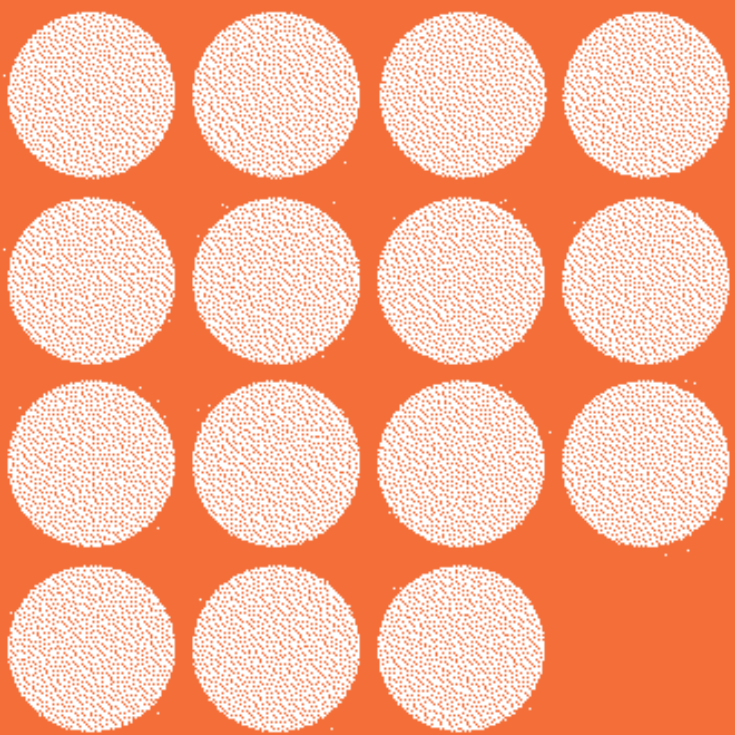
TOM II



Innowacje

Publikacja towarzysząca debacie „Prawo do cyfrowego wykluczenia. Godność i prywatność a rozwój nowych technologii" zorganizowanej przez kancelarię Wardyński i Wspólnicy w ramach obchodów jej 30-lecia.

Redakcja merytoryczna: Krzysztof Wojdyło
Redakcja: Justyna Zandberg-Malec

Spis treści

Tomasz Wardyński
Krzysztof Wojdyło

Technologia jako źródło wyzwań

Każda nowa technologia znajdująca powszechne zastosowanie zmienia istniejący świat. Przeobrażenia następują niezauważalnie, lecz dogłębnie. Powstaje pytanie, jak w nowej rzeczywistości chronić rządy prawa, wartości istotne dla społeczeństwa obywatelskiego i prawa osób.

Na naszych oczach narodziła się nowa rzeczywistość gospodarcza funkcjonująca w cyberprzestrzeni. Ludzkie działania – zarówno te pozytywne, jak i negatywne – przenoszą się do przestrzeni wirtualnej, która funkcjonuje ponad granicami państw. Dlatego musimy rozwijać umiejętność stosowania znanych nam instytucji prawa w odniesieniu do nowej rzeczywistości.

Od kilku lat w naszej kancelarii działa interdyscyplinarna praktyka prawa nowych technologii. Wchodzących w jej skład prawników łączy pasja rozpoznawania zagadnień technicznych i ich wpływu na możliwość skutecznej ochrony praw obywateli i społeczeństwa obywatelskiego – a także przekonanie, że prawnicy powinni zwiększyć zainteresowanie nowymi technologiami.

Czas technologicznej rewolucji

Innowacyjność jest dziś słowem-kluczem organizującym życie społeczne i gospodarcze. Rządy i przedsiębiorstwa tworzą strategie innowacji. Startupy skupiają bezprecedensową uwagę. W szumie informacyjnym łatwo przegapić głębszy sens postępujących przeobrażeń.

Technologie zmieniają nas w sposób fundamentalny. Nie są neutralne społecznie, gospodarczo oraz kulturowo. Biorąc pod uwagę dynamikę oraz skalę zmian, refleksja nad nowymi technologiami jest nadal niewystarczająca. Rezygnując z pogłębionej refleksji, ryzykujemy, że wiele zmian dokona się niepostrzeżenie, pozbawiając nas szansy na ewentualną reakcję.

Jako prawnicy za szczególnie istotne uważamy prawidłowe uchwycenie wzajemnych relacji prawa i technologii. Wiemy, że przed prawem stoją

w najbliższych latach olbrzymie wyzwania polegające na konieczności uregulowania sztucznej inteligencji, blockchaina czy inżynierii genetycznej. Nie chodzi o proste uregulowanie nowej dziedziny rzeczywistości. Duża część nowych technologii może fundamentalnie zmienić paradygmaty będące podstawą współczesnych systemów prawa. Mogą zmienić znaczenie prawa, sposób jego tworzenia oraz egzekwowania. Niechybnie zmieni się również sposób wykonywania zawodu prawnika. Zmienić się zatem będziemy musieli także my – prawnicy.

Prawo w ciągłej pogoni za rzeczywistością

Wzajemne relacje prawa i nowych technologii kwituje się zwykle stwierdzeniem, że prawo nie nadąża za rzeczywistością. Nawet jednak w tej obserwacji kryje się bardzo istotna prawda. Coraz więcej jest obszarów rzeczywistości, które nie są przez prawo skolonizowane.

Przyzwyczailiśmy się żyć w świecie, w którym zdecydowana większość obszarów naszej aktywności podlega regułom usankcjonowanym przez tradycyjnego ustawodawcę. Taki stan rzeczy może budzić frustrację, ale też daje poczucie pewności, stabilizacji i kontroli nad rzeczywistością. Oddając pole nowym technologiom, zaczynamy tę kontrolę zatracać.

Nie chodzi o to, że w nowych obszarach rzeczywistości nie ma w ogóle reguł. Są one jednak tworzone inaczej, niż przywykliśmy. Najważniejsze zasady działania internetu, do dziś wpływające na jego kształt, nie były wytworem tradycyjnie rozumianego ustawodawcy posiadającego demokratyczną legitymację społeczną do stanowienia prawa. Nie były też przedmiotem demokratycznej debaty publicznej.

W nowych obszarach rzeczywistości rośnie znaczenie norm technicznych oraz instrumentów tzw. soft law, takich jak zalecenia, rekomendacje, dobre praktyki. Wydaje nam się bardzo ważne, aby prawnicy uświadomili sobie ten proces i odpowiednio szybko zaczęli aktywnie partycypować w alternatywnych działaniach prawotwórczych.

Postępująca komplikacja systemu i wewnętrzne sprzeczności

Wraz z postępem technologii postępuje również komplikacja systemu prawnego. Każda nowa dziedzina prędzej czy później staje się przedmiotem regulacji, tworzonych bądź tradycyjnie, bądź w sposób alternatywny. Jeszcze trzydzieści lat temu nie było regulacji dotyczących internetu. Dwadzieścia lat temu przepisy dotyczące elektronicznych usług płatniczych były szczątkowe. Dzisiaj ten ostatni obszar jest regulowany kilkudziesięcioma aktami prawnymi i setkami przepisów prawa.

W konsekwencji rośnie liczba wzajemnych powiązań oraz konfliktów pomiędzy poszczególnymi elementami systemu. Regulacje tworzone w oderwaniu od szerszego kontekstu prowadzą do wewnątrzsystemowych sprzeczności. Takich sytuacji będzie zapewne coraz więcej.

System targany wewnętrznymi sprzecznościami nie może zapewnić poczucia bezpieczeństwa prawnego oraz sprawiedliwości. Obsługa prawna będzie coraz droższa i coraz mniej efektywna. Rozstrzyganie sporów sądowych będzie coraz bardziej czasochłonne i będzie wymagało angażowania kosztownych ekspertów. Na krótką metę taka sytuacja jest atrakcyjna dla prawników. Długoterminowo jednak jest bardzo niekorzystna dla społeczeństwa i gospodarki. Pomoc prawna może w jeszcze większym stopniu stać się dostępna tylko dla nielicznych.

Stajemy zatem przed pytaniem o model dalszego rozwoju systemu prawa. Model dotychczasowy w uproszczeniu sprowadza się do tworzenia kolejnych regulacji w reakcji na rozwój nowych technologii. Prowadzi to do dalszego rozrostu i komplikacji systemu prawa, czyniąc go coraz mniej przejrzystym. Grozi to utratą kontroli nad całością systemu i wzrostem społecznej frustracji wywołanej brakiem przejrzystości systemu prawa.

Dlatego należy pilnie podjąć twórczy wysiłek w celu wypracowania rozwiązań alternatywnych. W grę może wchodzić zarówno odejście od dotychczasowego paradygmatu, zgodnie z którym prawo musi szczegółowo regulować każdy nowy obszar rzeczywistości, jak i rozwój narzędzi (np. opartych na sztucznej inteligencji) pozwalających skuteczniej identyfikować wewnątrzsystemowe sprzeczności.

Wyzwanie 1: blockchain

Blockchain ma potencjał stworzenia prawdziwie globalnej przestrzeni wymiany dóbr i usług, w której – z uwagi na jej architekturę – nie ma suwerena. Blockchain jest bowiem rozproszonym rejestrem utrzymywanym przez niezależne od siebie podmioty rozmieszczone po całym globie, nad którymi – co do zasady – nikt nie sprawuje kontroli.

Można powiedzieć, że to, co dzieje się na blockchainie, dzieje się wszędzie i nigdzie zarazem. Nie sposób wskazać konkretnego porządku prawnego, który reguluje poszczególne czynności czy transakcje, które się w tej przestrzeni rozgrywają.

Przy okazji należy wspomnieć o dynamicznym rozwoju smart kontraktów. Tym mianem określa się stosunki prawne uregulowane nie za pomocą tradycyjnego kontraktu pisanego językiem naturalnym, lecz za pomocą kontraktu, który ma postać kodu. Taki kontrakt może być zawierany i egzekwowany

w sposób automatyczny. Rozwiązania oparte na smart kontraktach są powszechnie wykorzystywane na blockchainie.

Blockchain stawia wiele wyzwań przed tradycyjnym systemem prawa. W tej swoistej nowej jurysdykcji, w której coraz częściej to kod jest prawem, trzeba stworzyć gwarancje bezpieczeństwa i sprawiedliwości. Prawnicy mają tu do odegrania bardzo istotną rolę. Aby jej jednak sprostać, będą musieli porzucić wiele dotychczasowych przyzwyczajeń i nabyć zupełnie nowe umiejętności.

Wyzwanie 2: autonomiczne algorytmy

Już dzisiaj algorytmy są współuczestnikami wielu procesów decyzyjnych. Przetwarzają ogromne ilości danych i podejmują decyzje w czasie nieosiągalnym dla człowieka. Wraz z rozwojem technologii zwiększają przy tym stopień autonomii. I to właśnie rodzi najwięcej wyzwań dla systemu prawa.

Logika podejmowania decyzji przez autonomiczne algorytmy często jest dla ludzi nieznana lub niezrozumiała. Mimo to, z uwagi na efektywność tych algorytmów, jesteśmy gotowi oddać im kontrolę nad wieloma obszarami rzeczywistości. Już dziś algorytmy oceniają zdolność kredytową lub podejmują decyzje inwestycyjne. W najbliższej przyszłości oddamy im kontrolę nad transportem, usługami logistycznymi, a nawet usługami medycznymi.

Algorytmy – jako nowy czynnik/aktor współtworzący naszą rzeczywistość – mogą stać się swoistym podmiotem praw i zobowiązań. Ich działań nie sposób jednoznacznie przypisać konkretnym osobom. Nawet bowiem twórcy autonomicznych algorytmów nie są w stanie przewidzieć ich logiki i zachowań.

W ciągu najbliższych lat system prawa będzie musiał się odnieść do tego fenomenu. Wydaje się, że nie sprawdzi się tradycyjne podejście polegające na znalezieniu czynnika ludzkiego, który może zostać powiązany z autonomicznym algorytmem i wziąć odpowiedzialność za jego działania. Musimy poszukać rozwiązań niestandardowych, które oddadzą naturę nowych aktorów naszej rzeczywistości.

Wyzwanie 3: cyberprzestępczość

Choć o nowych cyberprzestępstwach dowiadujemy się niemal codziennie, wciąż nie uświadamiamy sobie do końca znaczenia tego zjawiska. Cyberprzestępczość bardzo dobitnie obnaża bezsilność tradycyjnego systemu prawa w dobie nowych technologii. Wykrywalność cyberprzestępstw pozostaje bardzo niska. Bardzo duża liczba postępowań kończy się umorzeniem z powodu niewykrycia sprawcy.

Składa się na to wiele czynników. Po pierwsze, cyberprzestępstwa mają z reguły charakter międzynarodowy, co wymaga skoordynowanych działań organów ścigania z wielu jurysdykcji. Tymczasem system międzynarodowej

pomocy prawnej w wielu takich sprawach jest bardzo nieefektywny, przez co ofiary cyberprzestępstw muszą ponosić ogromne koszty obsługi prawnej, bez gwarancji sukcesu. Po drugie, walka z cyberprzestępczością wymaga wysoce specjalistycznej wiedzy, a zasoby odpowiednich specjalistów są ograniczone. Przekłada się to na ogromne koszty sporządzania dowodów i ekspertyz, a także na przewlekłość postępowań.

Niska wykrywalność cyberprzestępstw oraz rosnąca liczba ich bezsilnych i pozostawionych samym sobie ofiar dowodzi swoistego regresu cywilizacyjnego i prawnego. Tu również pilnie potrzebna jest zmiana paradygmatu i sposobu działania, gdyż tradycyjne metody zawodzą i nie ma widoków na poprawę sytuacji w najbliższej przyszłości. Bez nowego podejścia grozi nam rosnące poczucie anarchizacji, a nawet odwrót od nowych technologii.

Wyzwanie 4: prawnicy w nowej rzeczywistości

Spodziewamy się, że znacznie bardziej niż dotychczas w wykonywaniu zawodu będą nas wspierać zautomatyzowane rozwiązania. Odnalezienie odpowiedniej normy prawnej czy jej odpowiednie przypisanie do określonego stanu faktycznego będzie dzięki nim łatwiejsze. Być może wkrótce proces ten będzie w dużej mierze przebiegał w ogóle bez udziału prawników. Zmieni się więc istota naszego zawodu.

Kluczowa stanie się umiejętność dekodowania głębszego, humanistycznego sensu rzeczywistości. To właśnie w tym procesie upatrujemy istoty zawodu prawnika w przyszłości. Tylko dzięki perspektywie humanistycznej będziemy w stanie regulować nowe obszary rzeczywistości w sposób, który zapewni zachowanie ludzkiej godności oraz sprawiedliwości. Tylko perspektywa humanistyczna umożliwi nam holistyczne spojrzenie na rzeczywistość oraz identyfikację sensu i znaczenia coraz bardziej skomplikowanych norm prawnych.

Wykształcenie powyższych umiejętności będzie niewątpliwie wymagało zmiany sposobu kształcenia prawników. Coraz mniejsze znaczenie w procesie kształcenia powinno odgrywać pamięciowe przyswajanie prawa. To strata energii, bo w odnajdywaniu przepisów prawa będą nam pomagać maszyny. Znacznie większy nacisk powinniśmy za to kłaść na procesy, które uczą prawników rozumienia rzeczywistości, pobudzają w nich pasje poznawcze oraz przybliżają humanistyczną perspektywę patrzenia na świat. Proces kształcenia powinien też zapewnić zasób wiedzy i umiejętności niezbędnych do zrozumienia technicznych aspektów działania nowych technologii.

Konkluzje

Naszą zawodową powinnością jest dbałość o zachowanie i utrzymanie w otaczającej nas rzeczywistości podstawowych wartości, do których zalicza

się m.in. ludzka godność oraz sprawiedliwość. Tradycyjnie przyjmowaliśmy, że zagrożenia dla tych wartości pochodzą przede wszystkim ze strony opresyjnych systemów politycznych. Dynamiczny rozwój techniki stworzył tymczasem dodatkowe źródło zagrożeń, które pozostawione samemu sobie może doprowadzić do stworzenia rzeczywistości zdehumanizowanej.

Dlatego jako prawnicy musimy zwiększyć nasze zainteresowanie nowymi technologiami. Aby sprostać wyzwaniom, które technologia stawia przed społeczeństwami, kulturą oraz polityką, potrzebny jest zbiorowy wysiłek środowiska prawniczego, nakierowany na wytwarzanie u prawników nowych umiejętności oraz nowego podejścia do wykonywania zawodu.

Tomasz Wardyński
adwokat, wspólnik założyciel kancelarii

Krzysztof Wojdyło
adwokat, wspólnik odpowiedzialny za praktykę prawa nowych technologii

Agnieszka Kraińska

Wolność od internetu

Wolność dostępu do sieci internet i wolność w sieci są gwarantowane w prawie UE między innymi poprzez zasadę neutralności internetu. Internet jest traktowany jako usługa publiczna, a brak uprzywilejowania przekazu gwarantuje równy dostęp do treści. Prawo dostępu do internetu jest wyrazem prawa człowieka do wolności opinii i wyrażania jej (ujętego w art. 19 Powszechnej Deklaracji Praw Człowieka oraz art. 10 Europejskiej Konwencji Praw Człowieka), którego doniosłość nie podlega dyskusji.

Nie można jednak zapominać o drugiej stronie internetu, czyli o zbieraniu danych użytkowników na masową skalę. Takie dane mają ogromną wartość i mogą być wykorzystane na wiele sposobów, również przez administrację publiczną, która coraz częściej sięga po technologie informatyczne i telekomunikacyjne. Pod hasłem e-administracji kryją się zagadnienia związane z e-tożsamością, e-dowodami, technikami skanowania twarzy, siatkówki i linii papilarnych. Biorąc pod uwagę ryzyka związane z wykorzystaniem tych danych, kusząca wydaje się koncepcja uprawnienia do odmowy udziału w internecie, wolności od internetu. Czy realizacja takiego prawa w ujęciu negatywnym jest w ogóle możliwa albo czy jeszcze będzie możliwa w bliskiej przyszłości?

Teza o prawie do tak rozumianej wolności może brzmieć dość kontrowersyjnie, szczególnie w świecie, w którym uwaga rządów, organizacji pozarządowych oraz organizacji międzynarodowych takich jak Unia Europejska czy ONZ skupia się raczej na problemie wykluczenia cyfrowego. Postaram się jednak udowodnić, że postulat wolności od internetu jest jak najbardziej uzasadniony. Za jedną z gwarancji takiej wolności uznać można prawo do prywatności zawarte w art. 12 Powszechnej Deklaracji Praw Człowieka oraz art. 8 Europejskiej Konwencji Praw Człowieka.

Prywatność i wolność

Wiele powieści i filmów straszy nas dystopijnym społeczeństwem pozbawionym prywatności. Prywatność ma bowiem fundamentalne znaczenie

nie tylko w wymiarze indywidualnym, ale również dla istnienia liberalnej demokracji.

Osobowość każdego z nas jest kształtowana społecznie od najmłodszych lat. Indywidualność i jej rozwój wymaga jednak przestrzeni prywatności i umiejętności stawiania granic. Subiektywna podmiotowość oraz zmysł krytyczny kształtują się pomiędzy sferą publiczną a prywatną. Nie bez powodu systemy totalitarne dążą do ograniczenia sfery ludzkiej prywatności do minimum. Nieustanna kontrola nad jednostką daje możliwość stałego kształtowania jej zachowań i formowania osobowości.

Tymczasem współczesna cywilizacja techniczna jest coraz bardziej cywilizacją rozproszonej uwagi i permanentnego bodźcowania, gdzie nie ma czasu na chwile skupienia. Otaczająca nas rzeczywistość naszpikowana jest elektronicznymi urządzeniami monitorującymi naszą codzienną aktywność i preferencje. W portalach społecznościowych dobrowolnie udostępniamy informacje na temat ogromnych obszarów życia.

Wciąż nie wszyscy użytkownicy internetu zdają sobie sprawę, że ich aktywność w sieci kształtuje informację zwrotną, którą z niej otrzymują. Wyszukiwarki filtrują i hierarchizują wyniki, dopasowując je do tego, co jest im wiadome o wyszukującym. W tym sensie zarówno wyszukiwarki, jak i grono znajomych na portalu społecznościowym, z którymi dzielimy wspólny światopogląd, utwierdzają nas w przekonaniu, że świat jest właśnie taki, jaki myślimy, że jest. Narzędzie, którym się posługujemy do poznawania otaczającego nas świata, kształtuje nasz sposób rozumienia tego świata.

Dane, które pozostawiamy w sieci, umożliwiają dopasowanie wyników wyszukiwania do naszych potrzeb i preferencji. Z całą pewnością jest to wygodne. Warto jednak pamiętać, że przenosząc aktywność do internetu i przypisując coraz większe znaczenie portalom społecznościowym, ryzykujemy utratą trzeźwego osądu na temat otaczającej nas rzeczywistości.

Dobrowolne wyrzeczenie się prywatności na rzecz wygody i bezpieczeństwa prowadzi do ograniczenia możliwości kształtowania krytycznego myślenia i niezależności – czyli w pewnym sensie do wyrzeczenia się wolności.

Prywatność a społeczeństwo demokratyczne

Sfera komfortu, którą generuje dla nas globalna sieć, nie jest za darmo. Płacimy za nią informacjami na nasz temat. W wymiarze indywidualnym rezygnacja z prywatności może usypiać ostrożność, krytycyzm i kreatywność. W wymiarze społecznym ma ona również donośne skutki.

Społeczeństwa demokratyczne nie mogą istnieć bez świadomego i aktywnego obywatela. Obywatel kształtuje instytucje polityczne i gospodarcze, a instytucje te kształtują jego i społeczeństwo, w którym żyje. Państwa

rezygnacja z prywatności może usypiać ostrożność, krytycyzm i kreatywność

liberalnej demokracji oraz instytucje gospodarki rynkowej są wytworem wieloletnich procesów i doświadczeń, a ich obywatele przyjmują za naturalne normy i zasady rządzące takimi społeczeństwami. Wielorakie przykłady wskazują, że nie da się przeszczepić liberalnej demokracji społeczeństwom, które nie są jeszcze na to gotowe.

Zmiana technologiczna wprowadzona przez internet umożliwiła bezprecedensowe zmiany w dostępie do informacji oraz do technologii komunikacyjnych. Te nowe narzędzia kreowane są przez nas, ale również nas formują – w tym sensie, że postrzegamy otaczający nas świat za ich pośrednictwem. Żeby sobie unaocznić taki wpływ, wystarczy porównać podróż samochodem z nawigacją GPS i bez tej nawigacji. Badania naukowe wykazują, że używanie urządzeń elektronicznych zmienia funkcjonowanie mózgu, a osoba korzystająca z elektronicznego urządzenia inaczej funkcjonuje w życiu codziennym.

Na dodatek coraz powszechniej posługujemy się narzędziami, których zasad działania kompletnie nie rozumiemy. Urządzenia te, dzięki połączeniu z internetem, dają możliwość stałego nadzoru i monitorowania ludzkiej aktywności. Nadzór taki nie jest przy tym związany z totalitarnym systemem politycznym, lecz z rozwojem kapitalizmu (wymiar komercyjny informacji) i współczesnego państwa narodowego (polityka bezpieczeństwa).

Dzięki rozproszonemu internetowi rzeczy oraz internetowi ludzi wspomniany nadzór nad ludzką aktywnością staje się wszechobecny, rutynowy i systematyczny, a rodzaj i intensywność tego nadzoru kształtowane są właśnie w odpowiedzi na tę aktywność.

Słusznie wskazuje się, że tego typu dyskretny i stały nadzór jest znacznie skuteczniejszy niż jawny i brutalny nadzór w państwach niedemokratycznych. Zresztą państwa niedemokratyczne chętnie wykorzystują nowoczesne narzędzia i wprowadzają stały monitoring społeczeństwa, jak wskazują na przykład ostatnie doniesienia o szerokim wykorzystaniu technik rozpoznawania twarzy w Chinach.

Państwa liberalnych demokracji gromadzą i wykorzystują dane rutynowo w celach bezpieczeństwa narodowego, czego dowodzą chociażby postępowania wszczynane przeciwko rządowi brytyjskiego przez organizację Privacy International (np. w sprawie masowego pozyskiwania danych telekomunikacyjnych przez brytyjskie służby wywiadowcze).

Informacje na nasz temat są także bezcenne w sensie komercyjnym, a apetyt na dane firm takich jak Google czy Facebook jest niezaspokojony. Informacje o preferencjach konsumenta służą do profilowania reklam, wyników wyszukiwania i innych treści, są one także odsprzedawane dalej. Dane pozostawiane w sieci są bardzo przydatne do konstruowania cen, zarządzania ryzykiem czy profilowania potencjalnych klientów.

W tym kontekście uderzające jest, że w społeczeństwach zachodnich konsumenci dobrowolnie i aktywnie biorą udział w tak rozumianym procesie nadzoru. Wystarczającą rekompensatą za ograniczenie sfery prywatności jest personalizacja informacji, poczucie bezpieczeństwa, dostęp do lepszych towarów i ciekawszych ofert czy wyższa pozycja w hierarchii na portalu społecznościowym. Mówi się nawet o osobowości definiowanej jako permanentna obecność w mediach społecznościowych.

Z przyczyn, które podlegają analizie psychologów, obecność w sieciach społecznościowych bazuje na silnych emocjach. Nie sprzyjają one pogłębionej dyskusji, lecz sprowadzają ją do fali hejtu i lajków. Ponadto ograniczenie kontaktów pomiędzy ludźmi o odmiennych poglądach eliminuje dyskusję i ścieranie się opinii. Przestaje istnieć debata publiczna. Taka debata bowiem wymaga z jednej strony dyskomfortu, a z drugiej – pogłębionej refleksji. Tymczasem obywatele żyjący w spersonalizowanym bąblu, stale bodźcowani nowymi informacjami i obrazkami, nie mają ochoty brać udziału w takiej debacie, nie mają potrzeby wyjścia ze strefy komfortu i zasklepiają się w swoich „plemionach".

Co jeszcze poważniejsze, obywatele żyjący w świecie technologii cyfrowej nie tylko podlegają stałemu nadzorowi, ale są bardzo podatni na manipulację fałszywymi informacjami, na co wskazują takie afery jak Cambridge Analytica.

Utrata prywatności warunkującej krytyczne myślenie jest więc zagrożeniem dla demokracji liberalnej.

Prywatność a innowacyjność

Społeczeństwo, w którym brakuje debaty, a obywatele żyją w bąblach tworzonych przez portale społecznościowe, nie jest społeczeństwem sprzyjającym innowacjom.

Prywatność jest warunkiem koniecznym innowacyjności, albowiem innowacyjność wymaga krytycznego myślenia oraz przestrzeni do eksperymentowania i ponoszenia porażek. Innowacyjność wymaga zmierzenia się z problemem i kreatywnego rozwiązania tego problemu, wymaga spotkań z ludźmi, którzy myślą inaczej, oraz zetknięcia z nowymi ideami. Innowator nie może być poddany tyranii transparentności i permanentnej oceny związanej ze stałą aktywnością w sieci.

Wprawdzie pojawiają się opinie, że może istnieć innowacja bez innowatora – na przykład będąca wynikiem automatycznego przetwarzania ogromnej ilości danych. Nie należy jednak mylić narzędzia, jakim jest Big Data, z innowacją. To człowiek musi zakreślić zakres badania oraz zinterpretować i wykorzystać jego wyniki.

Co dalej?

Powyższe rozważania nie mają na celu wykazania, że internet jest zły. Przeciwnie, internet daje dostęp do informacji i wymiany myśli na niespotykaną skalę. Jednak jak każde narzędzie, a w tym przypadku narzędzie o światowym zasięgu, rodzi również nieprzewidziane ryzyka i zagrożenia. Rewolucja związana z powszechnym dostępem do internetu trwa dopiero dwadzieścia lat i wszyscy uczymy się tego, w jaki sposób oddziałuje on na nasze życie, na otaczające nas społeczeństwo i naszą rzeczywistość.

Zapewnienie powszechnego dostępu do internetu i technologii cyfrowych może paradoksalnie pogłębiać rozwarstwienia klasowe oraz prowadzić do ogromnych nierówności związanych z jakością informacji, do których ludzie mają dostęp, a także z posiadaniem i wykorzystywaniem danych pozyskiwanych od ludzi. Nie można zapominać o nieustannej presji spowodowanej z jednej strony komercyjnym wymiarem internetu i dążeniem do zniesienia neutralności rozumianej jako równy dostęp do informacji, a z drugiej strony polityką bezpieczeństwa i dążeniem do wszechobecnej kontroli. W rozmaitych aspektach wymiary te wzajemnie się przenikają.

Konsekwencją utraty prywatności oraz nierównego dostępu do informacji może być powstanie małej uprzywilejowanej grupy osób mającej władzę w sieci i olbrzymich rzesz ludzi manipulowanych, będących wyłącznie producentami danych dla systemu.

Nie sądzę, by w społeczeństwie zachodnim możliwe jeszcze było całkowite wyłączenie się z internetu bez wykluczenia z normalnego funkcjonowania. Jednakże bezkrytyczna cyfrowa inkluzja prowadzi do świata, w którym, jak to przedstawiono w dystopijnej powieści „Krąg" Dave'a Eggersa, „Sekrety to kłamstwa, dzielenie się to troska, a prywatność to kradzież".

Znalezienie złotego środka i właściwe postawienie granic jest ogromnym wyzwaniem dla demokratycznego społeczeństwa. Konieczna jest edukacja dotycząca krytycznej obecności w e-rzeczywistości oraz odpowiednia regulacja zapewniająca indywidualną i społeczną kontrolę nad pozyskiwaniem i przetwarzaniem danych przez państwo i przez sektor prywatny, jak też dająca gwarancję równego dostępu do informacji. W tym zakresie widzę przestrzeń do rozsądnej interwencji państwa i do współpracy międzynarodowej, bez której działania te nie odniosą pożądanych efektów. Państwa narodowe w mojej ocenie nie są w stanie same poradzić sobie z zagrożeniami, które tak jak sam internet są ponadnarodowe i ponadgraniczne.

Agnieszka Kraińska
radca prawny, praktyka prawa europejskiego

prywatność
jest warunkiem
koniecznym
innowacyjności

Pionierskie początki

Z Włodzimierzem Szoszukiem
rozmawia Justyna Zandberg-Malec

Dziś kancelaria doradza w sprawach dotyczących blockchaina, kryptowalut, cyberprzestępczości... A jak to wyglądało 30 lat temu?

Początki były zupełnie pionierskie. Zaczynaliśmy w czasie transformacji ustrojowej, w początkach demokracji i wolnego rynku. Polska otwierała się na inwestycje zagraniczne, stawała się atrakcyjnym rynkiem zbytu dla produktów, których tu nigdy nie było, oraz miejscem szybko rosnącego rodzimego przemysłu. Jako mała kancelaria stanęliśmy przed zalewem zleceń, które przychodziły z całego świata i dotyczyły wszystkich dziedzin prawa.

Na dodatek proces reformowania prawa nie nadążał za zmianami ustrojowymi. To stwarzało wyzwanie dla prawników.

Każde zlecenie przypominało szycie garnituru na miarę. Było to bardzo ciekawe, ale zabierało mnóstwo czasu. Dopiero po kilku podobnych sprawach, transakcjach, pierwszych procesach sądowych mogliśmy wykształcić pewien rzemieślniczy warsztat, co po osiągnięciu biegłości pozwalało czasem być artystą.

Czy w związku z tym atmosfera przypominała tę w startupie?

Do pewnego stopnia tak. Znaliśmy się na tym, co było trzonem naszej działalności, ale całe otoczenie biznesowe, wymogi rynku i klientów były dla nas nowością. Mieliśmy jednak to szczęście, że zachodnie kancelarie, które zlecały nam pracę, dzieliły się z nami swoim know-how. Na bieżąco uczyliśmy się, jak z nimi pracować, jak rozumieć cele biznesowe naszych nowych klientów, jak je dopasowywać do polskich realiów. Dopiero uczyliśmy się, jak wcielić się w rolę doradcy biznesowego. Wcześniej normą było to, że prawnik poruszał się w świecie przepisów, nie realiów gospodarczych.

Na szczęście było sporo możliwości, żeby podnieść kwalifikacje i nauczyć się warsztatu. Znając język, można było wyjechać na studia albo staż za granicę. Były organizacje fundujące stypendia, były programy wymiany. Prawnicy z Zachodu przyjeżdżali, żeby zobaczyć, jak sytuacja ewoluuje, myśmy jeździli

do firm zachodnich. Ja wyjechałem na kilka miesięcy do firmy brytyjskiej, potem amerykańskiej. Wróciłem z zupełnie inną wizją prowadzenia spraw i kancelarii.

Uczyliśmy się też nowego sposobu pisania. Kiedyś prawnicy uważali, że zanim przejdą do konkluzji, muszą klienta wykształcić prawniczo. Zacytować mu pięć artykułów, osadzić je w szerszym kontekście, wyjaśnić ich cel, a dopiero potem, budując napięcie, doprowadzić go do konkluzji ważnych dla niego biznesowo. I to zabierało masę czasu – i nam, i klientowi, i było w ogóle niepotrzebne. Dopiero na stażach zetknąłem się z zupełnie innymi tekstami, które pisząc o problemie, w ogóle nie cytowały artykułów. Podawały przesłanki, uwarunkowania, ale w oderwaniu od gęstej prawniczej materii. I to było rewolucją.

Takie edukacyjne pisanie zachowało rację bytu w przypadku sądów. Sędziowie też byli mało oswojeni z nową rzeczywistością, dlatego na przykład pierwsze pozwy o ochronę znaków towarowych były właściwie wykładem, czym jest znak towarowy, jaki jest zakres ochrony, jaki mamy katalog roszczeń, jak je możemy realizować. Musieliśmy subtelnie i elegancko wytłumaczyć sędziemu, jak ma sobie poradzić z pierwszą sprawą nowego rodzaju.

Powszechne były też wtedy opinie prawne. Jeżeli coś było wątpliwe albo nie do końca czytelne w polskim prawie, musieliśmy zasięgać opinii przedstawicieli doktryny, którzy pomagali nam bardziej przekonująco przedstawić nasz wywód sędziemu. Dziś to straciło rację bytu. Dziś również argumentacja przed sądem jest bardziej zwięzła i skoncentrowana na określonym problemie prawnym.

Jakie były realia pracy prawnika 30 lat temu?

Przede wszystkim pracowaliśmy w innym tempie, znacznie wolniejszym – co nie znaczy, że mieliśmy więcej czasu. Mnóstwo czasu pochłaniały czynności, które dziś są właściwie niezauważalne.

Pamiętam, jak musieliśmy przetłumaczyć dużą umowę inwestycyjną, mającą kilkaset stron. Nie było wtedy jeszcze agencji tłumaczeń. Po prostu podzieliliśmy tę pracę między kilkanaście osób w kancelarii i pracowaliśmy w domu po nocach. Komputery już wtedy były, ale nie było poczty elektronicznej, która pojawiła się znacznie później. Teksty zapisywaliśmy na dyskietkach. Porozumiewaliśmy się za pomocą korespondencji papierowej i faksów. Rewolucją były kserokopiarki, które upowszechniły się w połowie lat 80. Nie było oczywiście internetu, który – wraz z pocztą elektroniczną – pojawił się w firmie dopiero w 1998 roku. Minęło jednak dobrych parę lat, zanim pojawiły się w nim

użyteczne treści. Dopiero w 2003-2004 r. dostęp do internetu faktycznie zaczął oznaczać szybki dostęp do danych i informacji z całego świata. Wtedy tempo pracy w naturalny sposób wzrosło. Na dodatek firma rozwijała się w tempie lawinowym i mieliśmy tyle roboty, że nie mogliśmy jej przerobić.

A jak wyglądały początki praktyki własności intelektualnej?

Na początek muszę wspomnieć o zmarłej w tym roku prof. Irenie Wiszniewskiej-Białeckiej[1], która budowała ten dział. Ja dołączyłem po dwóch latach jej działalności i przez wiele lat pracowaliśmy razem. Szybko też dołączyły kolejne osoby.

Pierwsze sprawy z naszej dziedziny były o tyle fascynujące, że polski rynek został zalany produktami z innych krajów. To był import zupełnie dziki, niezorganizowany, nie było jeszcze kanałów dystrybucyjnych. I natychmiast pojawiły się towary naruszające prawo autorskie czy prawa własności przemysłowej. Znaki towarowe i zasady uczciwej konkurencji były naruszane masowo. I musieliśmy – w imieniu naszych nowych klientów – bronić tych praw. Wszczynaliśmy pierwsze procesy o ochronę znaków towarowych. Próbowaliśmy wykorzystać instrumenty przewidziane w postępowaniu cywilnym, takie jak zabezpieczenie powództwa. To były rzeczy nieobecne w polskiej praktyce. W okresie powojennym do 1989 r. był tylko jeden proces o ochronę znaku towarowego. Sąd zarządził wówczas zabezpieczenie powództwa poprzez zajęcie towarów naruszających amerykański znak towarowy stosowany dla odzieży. Dziś w ciągu roku składamy co najmniej kilkanaście wniosków o zabezpieczenie. To pokazuje, że ochrona własności intelektualnej zaczynała się właściwie od zera.

Poziom świadomości społecznej był też chyba znacznie mniejszy. To były przecież czasy kaset sprzedawanych z łóżek polowych i oficjalnie działających punktów zajmujących się kopiowaniem płyt.

Oczywiście, piractwo szalało, rynek był tak zgłodniały, że właściwie wszystko można było sprzedać. Naruszyciele korzystali z momentu próżni, wykorzystywali okres opieszałej ochrony. Nie mogli też wiedzieć, czy firma, której prawa naruszają, będzie w Polsce chronić swoją własność intelektualną. Taki stan utrzymywał się do połowy lat 90. Potem ochrona bardzo szybko nabrała impetu i osiągnęła pułap porównywalny z tym w krajach rozwiniętych.

1 Prof. Wiszniewska-Białecka od początku 2001 r. została powołana jako sędzia Naczelnego Sądu Administracyjnego, a następnie w latach 2004-2016 była sędzią Sądu I Instancji działającego w ramach Trybunału Sprawiedliwości UE w Luksemburgu.

Polska przed akcesją musiała dostosować swoje ustawodawstwo do standardów unijnych, więc reforma prawa postępowała szybko. Dziś polscy sędziowie i polskie sądy ferują doskonałe rozstrzygnięcia, z których nierzadko korzystają nasi koledzy na Zachodzie.

A kiedy pojawili się polscy klienci? Bo rozumiem, że na początku to byli głównie zachodni właściciele praw.

Akurat w moim obszarze polscy klienci pojawili się dość późno. Ale potem gdzieś od 2000 r. polski biznes zaczął szybko reagować w nowym otoczeniu ekonomicznym i zaczęły powstawać prężne polskie firmy, które bardzo szybko zyskiwały pozycję rynkową. Wiedziały, że w sporze z dużymi korporacjami muszą mieć należytą obsługę prawną, a ponieważ nas znali bardzo często ze strony przeciwnej, często korzystali z naszej pomocy. Mieliśmy wtedy przyjemną świadomość, że pomagamy rodzącej się polskiej gospodarce, polskiemu biznesowi.

To wszystko brzmi dziś jak opowieść o zamierzchłych czasach. Dziwnie jest pomyśleć, że mówimy o realiach sprzed raptem kilkunastu lat. Dziś młodzi prawnicy są znacznie lepiej przygotowani do swojej roli. Co więcej, nie mogą polegać na swoistym kredycie, na którym polegaliśmy my. Wtedy klienci zdawali sobie sprawę, że w Polsce pewne rzeczy jeszcze się nie zorganizowały. Dziś inwestor spodziewa się od młodego polskiego prawnika tego samego, czego się spodziewa od prawnika w Belgii, Holandii czy Finlandii.

Oczywiste jest też to, że prawnik musi myśleć w kategoriach biznesowych. Największym komplementem dla prawnika jest usłyszeć od klienta „mój prawnik myśli tak jak ja".

Realia w dzisiejszym świecie – szczególnie w dziedzinie nowych technologii – zmieniają się coraz szybciej. Prawo z natury swojej pozostaje w tyle. Dlatego prawnicy muszą być gotowi na wciąż nowe wyzwania.

Włodzimierz Szoszuk
adwokat, wspólnik odpowiedzialny za praktykę własności intelektualnej

Rozmawiała Justyna Zandberg-Malec

największym komplementem dla prawnika jest usłyszeć od klienta „mój prawnik myśli tak jak ja”

Prawnicy w świecie nowych technologii

Z Tomaszem Wardyńskim
rozmawia Justyna Zandberg-Malec

Co się zmieniło w wykonywaniu zawodu prawnika w ciągu 30 lat istnienia kancelarii?

Wszystko i nic. Rolą adwokata – od początku istnienia tego zawodu, czyli od starożytnego Rzymu – jest przede wszystkim zaoszczędzenie klientowi stresu związanego z trudną sytuacją prawną, w której się znalazł przez swoje zaniedbanie, brak wiedzy albo nadużycie jego praw przez administrację czy kontrahenta. Z tego punktu widzenia nic się nie zmieniło. Natomiast oczywiście otoczenie zawodu zmieniło się diametralnie.

Dzisiaj wykonujemy nasz zawód w zupełnie innej rzeczywistości gospodarczej, społecznej i technicznej niż 15 czy 20 lat temu. Zmieniły się technologie, ale też potrzeby i oczekiwania klientów. Technologie generalnie ułatwiają pracę i oszczędzają czas, ale też przyspieszają rzeczywistość. Faks spowodował, że na listy zaczęliśmy odpowiadać tego samego dnia, a od wprowadzenia poczty elektronicznej na zapytania i korespondencję odpowiadamy w ciągu dwóch – czterech godzin, maksymalnie do końca dnia. I szybkość reakcji jest traktowana jako główny wyznacznik naszej jakości. A ponieważ szybko reagujemy, to mamy coraz więcej pytań, spraw i klientów. Wskutek zmiany technologicznej jesteśmy więc konfrontowani z ilością pracy, z którą nie poradzi sobie jedna osoba, dlatego zaczynamy działać w coraz większych zespołach.

Podobny efekt przyniosły duże transakcje gospodarcze, które wykształciły się na rynku, oraz wielkie procesy związane z tymi transakcjami. One też w jakimś sensie zmusiły ludzi, którzy wykonywali ten zawód w pojedynkę lub w małych zespołach, do powiększania tych zespołów, ponieważ problemy, jakimi przychodziło się zajmować, były wielodyscyplinarne. A jak wiadomo jeden umysł może dobrze opanować jedną – dwie dyscypliny. Gdy problem jest bardziej skomplikowany, potrzebne są konsylia. Kiedyś radziliśmy sobie w ten sposób, że dobierało się kolegów do spraw i robiło je wspólnie. Dzisiaj w prawniczym krajobrazie dominują duże firmy.

Oczywiście wielkość firmy również wpływa na sposób wykonywania zawodu. Większe firmy są bardziej korporacyjne niż mniejsze, trudniej

w nich utrzymać pewnego rodzaju ekskluzywną kulturę. A jak wiadomo różne są temperamenty ludzi i różnych szukają dla siebie sposobów wykonywania zawodu, różnej klienteli i tak dalej. Dlatego w naszym kraju – podobnie jak w Niemczech czy Francji – nadal istnieją praktyki indywidualne, w których adwokaci zajmują się tak jak kiedyś prawie wszystkim. A kiedy sprawa dotyczy dziedzin, którymi się nie zajmują, wysyłają klientów do kolegów i pilnują potem, jak ta praca jest wykonywana.

Ale widoczne są przede wszystkim firmy prawnicze ze względu na to, że poświęcają ogromne środki na reklamę i promocję, w związku z tym media huczą na ten temat. Media lubią sprzedawać sensację, która w odniesieniu do tego zawodu akurat jest szkodliwa. Ta celebrycka kultura dotknęła wiele firm prawniczych i wiele osób wykonujących ten zawód, w sprzeczności moim zdaniem z zasadami etyki zawodowej.

Z tego punktu widzenia można powiedzieć, że rozwój, któremu zawód podlega, ma dobre i złe strony, i tylko od ludzi zależy, w jaki sposób będą się w tym zmieniającym się świecie odnajdowali. Bo pamiętajmy, że na końcu to, kim chcemy być, to jest nasz osobisty wybór będący funkcją naszego wychowania, temperamentu, poczucia przyzwoitości, poczucia estetyki i poczucia odpowiedzialności za klientów i własną rodzinę.

A czy nowe technologie nie odwrócą tego trendu tak, że firmy będą maleć i upowszechni się model „kilku prawników plus sztuczna inteligencja"?

Jestem zdania, że duża część praktyki, którą firmy prawnicze dzisiaj wykonują, zostanie przejęta przez firmy technologiczne, które stworzą zautomatyzowane narzędzia i będą oferować ich usługi bezpośrednio klientom. Już dzisiaj mamy do czynienia z programami, które pozwalają na wykonywanie tej części pracy prawniczej, która jest pracą informacyjną i opiniotwórczą. Są automaty do konstruowania prostych umów i kompilowania odpowiedzi na proste pytania prawne. Z biegiem czasu – i wydaje mi się, że szybciej niż wolniej – będą one umiały się uporać z coraz bardziej skomplikowanymi zadaniami. Każdy rozwój napotyka na początku małe przeszkody, które są bardzo szybko usuwane. A gdy zostaną usunięte te zasadnicze, to postęp następuje lawinowo.

Uważam, że praca prawnika, również w firmie prawniczej, zostanie ograniczona do pracy najtrudniejszej, o największym wkładzie intelektualnym – czyli właśnie do pracy bezpośrednio z klientem, której celem jest pomoc w podejmowaniu decyzji w taki sposób, żeby nie wiązało się to ze stresem. Specjalistów mogą zastąpić maszyny, ale twórczą pracę, gdzie ta twórczość jest funkcją skomplikowanej sytuacji klienta – nie tylko ze względów prawnych,

ale również psychologicznych i emocjonalnych – wciąż wykonać może tylko człowiek, wspierany oczywiście przez technologię. W związku z tym myślę sobie, że w pewnym sensie zawód wróci do punktu wyjścia. Czyli będziemy robili to, co robili wielcy adwokaci, wielcy prawnicy i porządne firmy sto lat temu.

A co sprzyja innowacyjności – na poziomie firmy i gospodarki? I czy powinniśmy tę innowacyjność wynosić na piedestał?

Przede wszystkim musimy wiedzieć, co to jest innowacyjność. Najpierw jest idea, a potem są innowacje. Wydaje mi się, że dopóki nie ma się poukładanej aksjologii, czyli pewnych wartości, które muszą przyświecać naszemu działaniu w odniesieniu do rozwiązania problemu – bo nasza praca to jest rozwiązywanie problemów – to nie ma co się brać za innowacje. Innowacje są niczym innym jak wdrożeniem idei, czyli uruchomieniem funkcjonowania wartości. Trzeba wiedzieć, co się robi i dlaczego, a dopiero potem jak. A innowacja to jest know-how, czyli jak. I dla innowacji nie ma ograniczeń, ale trzeba pamiętać, że ludzie od innowacji nie zawsze są ludźmi od aksjologii.

Czyli niektórych innowacji lepiej nie wprowadzać?

Nie. Każde rozwiązanie techniczne, każda innowacja jest z aksjologicznego punktu widzenia indyferentna. Zaczyna mieć znaczenie dopiero wtedy, kiedy ludzie zaczynają ją stosować. I oczywiście kiedy jest wykorzystywana przez ludzi złej wiary, jest szkodliwa. Jeżeli jest wykorzystywana przez ludzi dobrej wiary, w zbożnym, społecznie użytecznym celu, jest pożyteczna. Nie technologie szkodzą, tylko ludzie, którzy się nimi posługują.

Oczywiście każdy wynalazek, który powoduje pewne zmiany, działa przez jakiś czas w sposób nierozpoznany. Musimy się nauczyć szybko rozpoznawać, jakie są efekty społeczne i kulturowe wprowadzanych innowacji. Cały system regulacji ustawić w taki sposób, żeby próbować eliminować te negatywne skutki, które one ze sobą niosą. I tak po jakimś czasie dochodzi do tego, że zabrania się przynoszenia do szkoły smartfonów w taki sam sposób, jak zabrania się w szkole palenia papierosów.

A czy regulacje powinny też zapobiegać kumulowaniu wpływów z tych technologii w ręku kilku osób na świecie?

Wracamy do zagadnienia ludzi złej i dobrej wiary. Neil Postman w książce „W stronę XVIII stulecia: Jak przeszłość może doskonalić naszą przyszłość" napisał, że każda zmiana technologiczna zmusza nas do zadania sobie kilku pytań: jaki problem rozwiązuje dana technologia, czyj jest to problem, kto

może najbardziej ucierpieć wskutek tej zmiany, jakie nowe problemy może ona wywołać oraz kto uzyska szczególną władzę ekonomiczną i polityczną w jej efekcie.

Trzeba sobie zdawać sprawę, do jakiego stopnia dany wynalazek może być wykorzystany w złej wierze i nadużyty przez jakąś grupę osób w celu kontrolowania społeczeństwa czy dostępu do udogodnień przyniesionych przez ten wynalazek. Oczywiście jest też pytanie, jak społeczeństwo obywatelskie ma się przed tym bronić. I to jest w tej chwili najistotniejsze. Bo technologie spowodowały również zmiany w demokratycznym systemie państwa prawa. Mechanizmy, które wymyślono jeszcze w XIX w., a krystalizowały się w połowie XX w., okazały się dysfunkcjonalne w zderzeniu z działalnością ludzi złej wiary posługujących się technologiami. I pytanie brzmi, kto zdąży pierwszy: czy obywatele, wprowadzając regulacje zapobiegające nadużyciom technologii, czy grupy, które się mobilizują właśnie po to, żeby opanować te technologie wyłącznie na swój użytek.

Ale chyba zawsze jest tak, że na początku nikt sobie nie zdaje sprawy z tego, jakie dany wynalazek może mieć skutki. Dopiero po jakimś czasie widać dokładnie, jak może zostać użyty – w celu pożytecznym społecznie i w celu społecznie szkodliwym. I wtedy muszą powstawać stosowne regulacje. To jest właśnie nadrzędny obowiązek prawników na najbliższe lata: zrozumieć zachodzące procesy technologiczne i sformułować jasne reguły pozwalające na zidentyfikowanie nadużyć oraz przypisanie odpowiedzialności za niewłaściwe korzystanie z technologii.

Przykładem są boty generujące fake newsy, powodując dysfunkcję systemów demokratycznych. Ludzie się zorientowali, że zostali zmanipulowani, i teraz należy się spodziewać kontrakcji, która wyeliminuje to negatywne zjawisko z życia społecznego. Oczywiście pojawią się następne problemy, przy okazji następnych wynalazków. Dlatego cały czas należy być czujnym, obserwować wpływ tych urządzeń na sposób funkcjonowania młodych ludzi, na edukację, ale trzeba też zdawać sobie jasno sprawę z tych wszystkich nieograniczonych możliwości, które te nowe technologie otwierają. Trzeba brać to, co dobre, a eliminować to, co złe. I tyle. Czyli na końcu wszystko nam się sprowadza do walki dobra ze złem. I pod tym względem nasz świat nie różni się niczym od tego, czym był tysiące lat temu.

Tomasz Wardyński
adwokat, wspólnik założyciel kancelarii

Rozmawiała Justyna Zandberg-Malec

czy powinniśmy innowacyjność wynosić na piedestał

Krzysztof Wojdyło

Sztuczna inteligencja jako wyzwanie

Systemy AI coraz śmielej kolonizują nasz świat. Stają się immanentnym elementem rzeczywistości, wywołując pilną konieczność stworzenia zasad dla ich funkcjonowania. Nie ma przy tym znaczenia, czy wizje sztucznej inteligencji przejmującej kontrolę nad ludźmi ziszczą się w przewidywalnym horyzoncie czasowym. Nie potrzebujemy realizacji aż tak radykalnych wizji, aby zrozumieć wyzwanie, przed jakim stanęliśmy. Nawet znacznie mniej spektakularne systemy AI kreują bardzo podobne wyzwania.

Autonomia

Rozwiązania oparte na sztucznej inteligencji cechują się kilkoma właściwościami, które powodują, że bardzo trudno jest stosować do nich istniejące i znane konstrukcje prawne. Systemy AI mogłyby być traktowane jako bardziej zaawansowany rodzaj oprogramowania, gdyby nie to, że część z nich cechuje się swoistą autonomią. Wprowadza ona zasadniczą jakościową zmianę wymuszającą zupełnie nowe i oryginalne podejście prawa do tych systemów.

Istnieje trudny do precyzyjnego zdefiniowania i uchwycenia moment, w którym efekt działania określonego systemu AI przestaje być objęty zakresem intencjonalnego i intelektualnego związku przyczynowo-skutkowego pomiędzy tym systemem a jego ludzkim twórcą. Rozważmy to na przykładzie algorytmu tworzącego cyfrowe obrazy imitujące styl genialnych malarzy.

Twórcy tych algorytmów ograniczyli się do stworzenia mechanizmu samouczącego, który po przeanalizowaniu odpowiedniej ilości danych jest w stanie zidentyfikować i imitować unikalny styl danego malarza. Dzieła wychodzące spod wirtualnego pędzla tego cyfrowego algorytmu nie są dziełami informatyków, którzy stworzyli samouczący się algorytm. Algorytm ten cechuje swoista autonomia, która powoduje rozerwanie związku pomiędzy stworzeniem algorytmu a stworzeniem obrazu. Na tej samej zasadzie

autonomia systemów AI wymusza zupełnie nowe podejście prawa

twórca narzędzia, nawet bardzo intelektualnie wyrafinowanego, np. procesora w komputerze, nie jest uznawany za twórcę dzieła wytworzonego z pomocą komputera wyposażonego w ten procesor. Oczywiście istnieje nierozerwalny i funkcjonalny związek przyczynowo-skutkowy pomiędzy twórcą procesora, procesorem, komputerem oraz dziełami wytworzonymi przez ten komputer, ale nie jest to związek, któremu przypisywalibyśmy jakieś zasadnicze znaczenie prawne.

Tym, co odróżnia przywołany przykład z procesorem od algorytmu malującego obrazy, jest brak czynnika ludzkiego we wskazanym łańcuchu zależności. Pomiędzy twórcą procesora a twórcą dzieła wytworzonego przez komputer używający tego procesora jest zazwyczaj jakiś człowiek, który skupia na sobie wiązkę praw związanych z dziełem wytworzonym z użyciem tego komputera. W przykładzie z malującym algorytmem nie ma tego elementu. Tu pomiędzy człowiekiem tworzącym algorytm a dziełem wytworzonym przez algorytm nie ma już żadnego elementu ludzkiego.

Algorytm jest więc narzędziem, które samo stało się twórcą. Uzyskało przymiot twórczego działania. Możemy ten fakt zlekceważyć, kierując się przywiązaniem do zastanych instytucji prawa. Będzie to jednak podejście negujące rzeczywistość, lekceważące zmianę, którą wnoszą do niej autonomiczne systemy AI. Przy takim podejściu prawo porzuci nowy wymiar rzeczywistości, abdykując z jego uporządkowania.

Podmiotowość

Swoista autonomia systemów AI jest przyczynkiem do dyskusji o prawnej podmiotowości tych systemów. Tradycyjnie to właśnie zdolność do autonomicznego działania uznawano za jeden z podstawowych przymiotów determinujących możliwość przyznania prawnej podmiotowości.

Rezultaty twórczej autonomii algorytmów mogą przedstawiać bardzo konkretną wartość ekonomiczną. Kluczowe staje się zatem rozstrzygnięcie, w ramach jakiego podmiotu kumuluje się wiązka praw i obowiązków związanych z dziełem wytworzonym przez system AI.

Brak bezpośredniego związku przyczynowo-skutkowego z działaniami człowieka powoduje, że nie jest wcale oczywiste, że wiązka ta powinna przypadać podmiotowi prawnemu rozpoznawalnemu przez aktualny system prawa. Nawet jeżeli opowiedzielibyśmy się za takim rozwiązaniem, należy jeszcze ustalić, jakiemu podmiotowi prawa należałoby przypisać tę wiązkę (twórcy algorytmu, posiadaczowi praw autorskich do algorytmu, a może dostawcy danych, za pomocą których algorytm zdołał wytworzyć swoją twórczą umiejętność?). Aktualny system prawa nie pozwala jednoznacznie tej wątpliwości rozstrzygnąć.

Z drugiej strony przyjęcie, że to sam algorytm powinien być uznany za nowy podmiot prawa, kreuje szereg istotnych trudności praktycznych. Algorytm musiałby w takim przypadku wchodzić w interakcje prawne z innymi podmiotami prawnymi. W wielu przypadkach byłoby to niemożliwe. Jakkolwiek bowiem algorytmy AI mogą cechować się swoistą twórczą autonomią, to niekoniecznie rozciąga się ona na składanie autonomicznych oświadczeń woli dotyczących rozporządzenia wytwarzanymi przez nie dziełami. Przynajmniej w odniesieniu do niektórych systemów AI oświadczenia te musiałyby być wydawane przez tradycyjne podmioty prawa. W tym kontekście pojawia się konieczność rozstrzygnięcia, jakie podmioty byłyby uprawnione do wydawania oświadczeń woli odnoszących się do danego algorytmu.

Wydaje się, że rozstrzygnięcie powyższych wątpliwości będzie wymagało interwencji ze strony ustawodawcy. Potrzeba takiej interwencji będzie coraz większa wraz z rozwojem systemów AI oraz wzrostem wartości wytwarzanych w sposób autonomiczny wytworów. Na kształt ostatecznego rozstrzygnięcia istotny wpływ będą miały również inne wyzwania, które stawiają przed prawem systemy AI.

Odpowiedzialność

Z podmiotowością prawną systemów AI wiąże się również problem odpowiedzialności za działania tych systemów. Logiczną konsekwencją przyznania, że swoista twórcza autonomia systemów AI powoduje zerwanie związku przyczynowo-skutkowego z działaniami człowieka, jest uznanie, że związek ten jest zerwany również w kontekście ewentualnej odpowiedzialności człowieka za działanie autonomicznego systemu.

Przypisywanie rozpoznawalnemu przez prawo podmiotowi prawa odpowiedzialności za działania, na które nie ma wpływu, byłoby niezgodne z podstawowymi zasadami odpowiedzialności cywilnej oraz karnej. W praktyce oczywiście rzeczywistość może być znacznie bardziej zniuansowana. Stopień autonomii systemów AI może być różny. W określonych przypadkach mogą pojawiać się przesłanki do przyjęcia, że rozpoznawany przez dzisiejsze prawo podmiot prawa przyczynił się w pewnym stopniu do działań danego systemu AI, co uzasadniałoby przynajmniej częściową odpowiedzialność.

Wydaje się, że również w tym przypadku niezbędna będzie interwencja ustawodawcy. Bez niej coraz bardziej istotny element naszej rzeczywistości, tj. rezultaty działań systemów AI, będzie dotknięty istotną systemową niepewnością.

z podmiotowością prawną systemów AI wiąże się problem odpowiedzialności za ich działania

Reguły nadzoru

Innym bardzo istotnym wyzwaniem jest ustalenie zasad nadzoru nad algorytmami. Prawo administracyjne służy – w dużym uproszczeniu – tworzeniu ram dla autonomii podmiotów prawa. W żadnym cywilizowanym porządku prawnym nie mamy do czynienia z nieograniczoną autonomią działania. Patrząc z tej perspektywy, autonomia systemów AI tworzy potencjalnie niebezpieczny systemowy wyłom.

Mając powyższe na uwadze, należy spodziewać się prób wprowadzenia administracyjnych regulacji dotyczących systemów AI. Nie będzie to zabieg prosty. Napotka on bowiem wiele technicznych oraz organizacyjnych trudności. Przede wszystkim rynek oprogramowania musiałby stać się rynkiem regulowanym, co jest niezgodne z dotychczasowym paradygmatem jego funkcjonowania. Dla wielu twórców oprogramowania kodowanie było i jest porównywalne z wolnością słowa. Uregulowanie kodowania byłoby trudne do zaakceptowania przez dużą część środowiska koderów.

Regulowanie rynku wymagałoby również stworzenia systemu, który pozwalałby wyspecjalizowanym organom administracji audytować algorytmy i wpływać na ich działanie, w sytuacji gdyby rezultaty autonomii algorytmów były sprzeczne z porządkiem prawnym danego państwa. Zarówno audytowanie, jak i możliwość ingerencji w algorytm może być jednak w określonych sytuacjach utrudnione.

Wiele algorytmów jest tworzonych jako tzw. „black boxy". „Logika" takich algorytmów wymyka się ludzkiej percepcji, tj. nie zawsze jesteśmy w stanie z góry przewidzieć, jak w danych okolicznościach zachowa się dany algorytm. To powoduje, że audytowanie tego rodzaju algorytmów jeszcze przed ich uruchomieniem jest zadaniem trudnym. Powracając do eksplorowanego w tym tekście przykładu algorytmu tworzącego obrazy, nie jesteśmy w stanie z góry przewidzieć, czy określony obraz wygenerowany przez algorytm nie będzie wypełniał znamion czynów zabronionych (np. czy nie będzie zawierał elementów pornograficznych).

W takich przypadkach szczególnie istotna jest możliwość administracyjnej ingerencji w działanie już funkcjonujących algorytmów. Jest to stosunkowo łatwe do wyobrażenia w przypadkach, w których algorytm funkcjonuje jako oprogramowanie działające w modelu scentralizowanym (np. oprogramowanie zainstalowane na urządzeniach należących do łatwego do zidentyfikowania podmiotu). Odpowiedni organ administracji może w takim przypadku podjąć określone działania wobec podmiotu, który posiada infrastrukturę, na której zainstalowany jest algorytm. Zdecydowanie większym wyzwaniem będzie ingerencja w algorytm, który funkcjonuje w zdecentralizowanym środowisku, np. jako smart kontrakt na publicznym blockchainie. W tym przypadku nie

ma łatwego do zidentyfikowania podmiotu, który może być adresatem działań administracji.

Prawa człowieka

Opisane powyżej wyzwania powodują, że systemy AI, niezależnie od swych potencjalnych zalet, tworzą również fundamentalne zagrożenia dla praw człowieka. Podstawowym źródłem tego zagrożenia jest autonomia systemów AI oraz ograniczony stopień kontroli nad nimi.

Do tej pory posługiwaliśmy się w tekście przykładem, który tworzy relatywnie niewielkie zagrożenie dla naszych praw i wolności. Można sobie oczywiście wyobrazić, że algorytmiczny malarz naruszy swoim dziełem godność konkretnych osób. Wpływ takiego naruszenia będzie jednak relatywnie niewielki w porównaniu z potencjalnie negatywnymi skutkami działania systemów AI angażowanych w procesy decyzyjne, które wpływają bezpośrednio lub pośrednio na sytuację prawną jednostek.

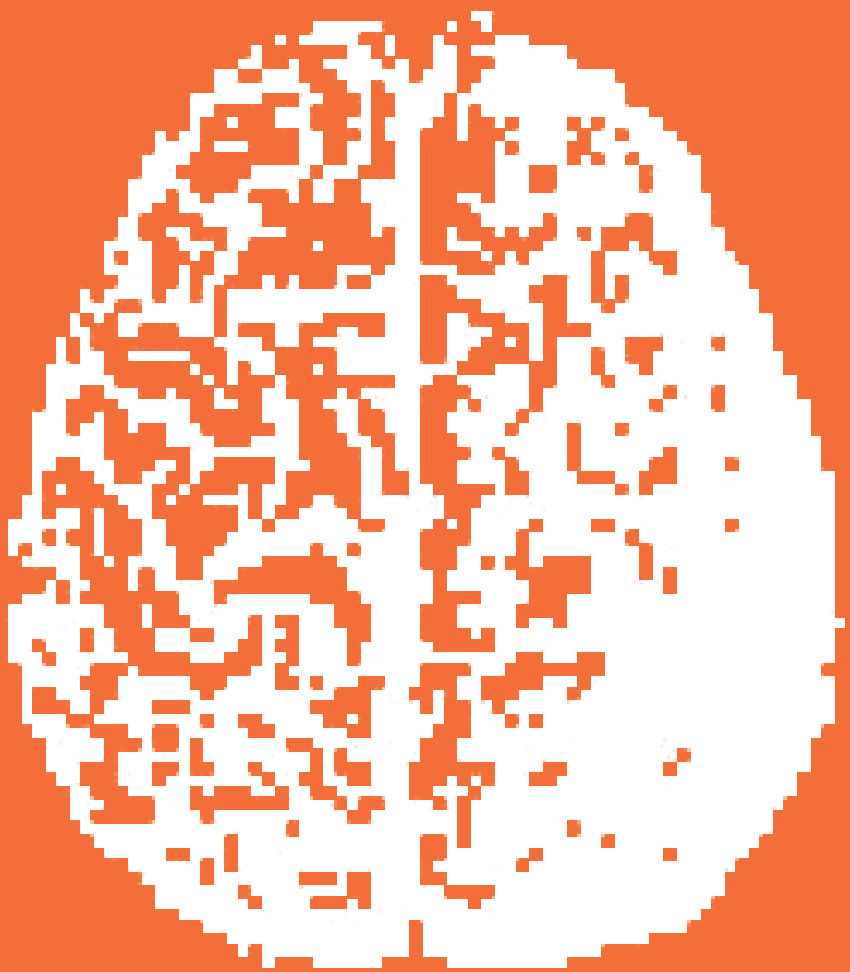
Z uwagi na dynamicznie postępującą komplikację rzeczywistości jest więcej niż pewne, że w podejmowaniu działań społeczno-gospodarczych będziemy w coraz większym stopniu wspierać się systemami AI. Są one w stanie znacznie efektywniej analizować znaczące zbiory danych niezbędnych do skutecznego zarządzania procesami społeczno-gospodarczymi. Efektem działania takich systemów AI mogą być rozstrzygnięcia, których adresatami są poszczególni ludzie. Tym samym systemy AI mogą mieć bezpośredni lub pośredni wpływ na kształtowanie sytuacji jednostek. Współczesny system prawa zawiera wiele zabezpieczeń, które skutkują tym, że w procesie wydawania rozstrzygnięć wpływających na sytuację prawną jednostek brane są pod uwagę podstawowe prawa człowieka, takie jak godność czy prawo do równego traktowania.

Tymczasem w przypadku systemów AI kryteria podejmowania rozstrzygnięć mogą być przedmiotem autonomii systemu. Nie mamy gwarancji, że podstawowe prawa człowieka są w tych kryteriach uwzględnione. Bierność wobec tego zagrożenia może spowodować, że w niedalekiej przyszłości oddamy, przynajmniej częściowo, kontrolę nad rzeczywistością systemom, dla których zapewnienie jednostce możliwości maksymalnej realizacji jej godności nie będzie nadrzędnym celem i kryterium działania.

Taka sytuacja oznaczałaby zasadniczą zmianę społeczno-kulturowego paradygmatu, w którym funkcjonujemy. Współczesny system prawa skupia swoją uwagę na jednostce. To jej prawa są punktem odniesienia przy kształtowaniu narzędzi, za pomocą których próbujemy zaprowadzić ład społeczno-gospodarczy. Jeżeli zależy nam na utrzymaniu takiego podejścia, musimy znaleźć sposób na zapewnienie, aby proces tworzenia systemów AI oraz nowa gospodarka oparta na tych systemach wpisały się w paradygmat praw człowieka. To, czy

sprostamy temu wyzwaniu, będzie miało zasadnicze znaczenie dla naszej przyszłości.

Krzysztof Wojdyło
adwokat, wspólnik odpowiedzialny za praktykę prawa nowych technologii



Jakub Barański
Łukasz Lasek

Cyberprzestępczość i nowy paradygmat odpowiedzialności

> „Jeżeli można coś spaskudzić, popsuć, zafałszować, ukraść, sprzeniewierzyć, złudzić, wystrychnąć na dudka, to niezależnie całkiem od tego, czy się taka działalność typu destrukcyjnego i występnego „aktywiście zła" opłaci, czy też dostarczy mu wyłącznie bezinteresownej satysfakcji, że przechytrzył zabezpieczenia, że zniszczył bez osobistego zysku to, co było dla innego cenne, można ze stuprocentową pewnością uznać, iż w nowych formach, nowej technologii, walka Arymana z Ormuzdem, zła z dobrem będzie się toczyła. A to, ponieważ tak było zawsze..."
>
> Stanisław Lem, Bomba megabitowa, Wydawnictwo Literackie 1999

Prowadzenie spraw karnych to jeden z najistotniejszych obszarów, w jakich kancelaria przez ostatnie trzydzieści lat świadczyła pomoc prawną. W tym czasie sposoby działania przestępców bardzo się zmieniły. Pod koniec lat 90. przestępczość kryminalna ustąpiła pola przestępczości gospodarczej. Od dobrych zaś kilku lat widać ewidentnie, że przestępczość jako taka przenosi się do cyberprzestrzeni. Z roku na rok liczba tradycyjnych przestępstw spada. Rośnie natomiast liczba przestępstw popełnionych z wykorzystaniem sieci informatycznych i komputerów.

Nie powinno to dziwić – im więcej życiowych czy biznesowych spraw załatwiamy przez internet, tym bardziej kuszącym środowiskiem staje się on dla różnego rodzaju przestępców. Od niedawna zainteresował również także tradycyjne zorganizowane grupy przestępcze, dotychczas zajmujące się handlem narkotykami czy karuzelami podatkowymi.

Przestępna działalność w cyberprzestrzeni jest relatywnie bezpieczna i tania. Mimo że każda działalność w sieci pozostawia cyfrowe ślady, wykrywalność cyberprzestępców jest bardzo niska. Przy tym działalność ta może

przynosić spektakularne zyski przy niewielkich inwestycjach. Przeprowadzenie popularnych w ostatnich latach oszustw przelewowych (*business email compromise*) czy ataków *ransomware* (blokowanie komputera i żądanie okupu za jego odszyfrowanie) nie wymagało od sprawców wybitnych umiejętności informatycznych. Wystarczyło wykupić w sieci odpowiednie oprogramowanie czy usługi.

Transgraniczna cyberprzestępczość i krajowy wymiar sprawiedliwości

Wzrost znaczenia cyberprzestrzeni nie umknął uwadze organów ścigania. Dziś już niemal każde państwo na świecie dysponuje wyspecjalizowaną komórką do walki z cyberprzestępczością. Wystarczy wspomnieć o utworzonych na przełomie 2016 i 2017 r. wydziałach ds. cyberprzestępczości w polskich jednostkach policji i prokuratury czy też o *European Cybercrime Center* Europolu (tzw. EC3) i *Internet Crime Complaint Center* amerykańskiego FBI (tzw. IC3). Jednostki te mają jednak charakter elitarny i służą do rozpracowywania najgroźniejszych grup przestępczych. Ograniczenia kadrowe i finansowe nie pozwalają na wykorzystywanie tych jednostek w większości przypadków cyberprzestępczości.

Sprawy cyberprzestępstw codziennie trafiają zatem na lokalne komisariaty, gdzie funkcjonariusze nie mają ani odpowiedniego przygotowania, ani odpowiednich środków technicznych, aby walczyć z cyberprzestępcami.

Cyberprzestępczość tymczasem, podobnie jak sam internet, ma najczęściej charakter transgraniczny, co utrudnia podejmowanie skutecznych działań śledczych organom przykutym do własnej jurysdykcji. Dla przykładu sprawcy tzw. oszustwa *phishingowego*, nawet jeżeli są obywatelami Polski i za cel obrali ofiarę z tego kraju, najprawdopodobniej działać będą za pośrednictwem serwerów znajdujących się w Izraelu czy Południowej Afryce, a wykradzione środki pieniężne przeleją na rachunki bankowe w Chinach czy Malezji. Po drodze skorzystają zapewne z pomocy podstawionych osób – tzw. słupów – pochodzących z kilku innych jurysdykcji. Transgraniczny przelew pieniędzy czy połączenia internetowe za pośrednictwem serwerów *proxy* zajmą przestępcom jedynie chwilę, natomiast z perspektywy polskich organów ścigania będą równoznaczne z co najmniej kilkumiesięcznym i bardzo zbiurokratyzowanym procesem pozyskiwania zagranicznej pomocy prawnej.

Choć zdarzają się spektakularne sukcesy w walce z cyberprzestępczością, dotyczą one głównie działań wielonarodowych zespołów, powołanych specjalnie w celu rozpracowania zorganizowanych grup przestępczych na poziomie

operacyjnym. Przykładem może być Operacja Triangle[1] przeprowadzona pod egidą Europolu i Eurojustu przez polskie Centralne Biuro Śledcze oraz organy ścigania z państw takich jak Włochy, Hiszpania, Belgia, Gruzja i Wielka Brytania. Szeregowi policjanci i prokuratorzy prowadzący śledztwa w sprawach indywidualnych mają raczej niewielkie szanse na wykrycie sprawców cyberprzestępstw, nie mówiąc już o ich schwytaniu. Ofiary cyberprzestępstw też nie mogą raczej liczyć na odzyskanie skradzionych im środków pieniężnych – tzw. *money trail* w cyberprzestrzeni jest równie trudny do tropienia jak sami sprawcy. Najczęściej sprawy zgłoszone na policję kończą się na zatrzymaniu i postawieniu zarzutów tzw. słupom, którzy otworzyli rachunek bankowy, wyrobili kartę SIM do telefonu albo dokonali innych czynności pomocniczych niezbędnych do popełnienia właściwego cyberprzestępstwa przez sprawców siedzących za ekranem komputera gdzieś daleko w innym kraju.

Międzynarodowe korporacje w walce z cyberprzestępczością

Większość cyberprzestępstw wymaga wykorzystania infrastruktury szeroko rozumianych dostawców usług krytycznych czy też instytucji zaufania publicznego, takich jak instytucje finansowe, operatorzy telekomunikacyjni albo platformy usług elektronicznych.

Najczęstsze cyberprzestępstwa są bowiem stosunkowo mało wyrafinowane pod względem informatycznym. W dużej mierze opierają się na socjotechnice, czyli technikach manipulowania ludźmi dzięki znajomości psychologii (w ten sposób popełniane są m.in. przestępstwa takie jak *phishing*, oszustwa typu *business e-mail compromise* czy ich wariant nazywany CEO *fraud*). Częściej można więc mówić o przestępstwach „cyberwspomaganych" (z ang. *cyber-facilitated*). Wymagają one od przestępców mniejszych nakładów finansowych i umiejętności niż przestępstwa zaawansowane pod względem technicznym (np. opierające się o złośliwe oprogramowanie, tzw. *malware*, sieci zainfekowanych komputerów, tzw. *botnety*, czy luki w systemach informatycznych, tzw. *zero-day exploits*), a odpowiednio przeprowadzone pozwalają na osiągniecie równie wysokich zysków.

W oszustwach opartych na socjotechnice wykorzystanie infrastruktury instytucji zaufania publicznego pozwala przestępcom zbudować wiarygodność w oczach potencjalnej ofiary. Kiedy e-mail z instrukcjami do przelewu wskazuje na rachunek w banku, który rzeczywiście istnieje i cieszy się rozpoznawalną marką, łatwiej podjąć decyzję o przelaniu nań swoich środków. Z drugiej

1 https://www.europol.europa.eu/newsroom/news/international-operation-dismantles-criminal-group-of-cyber-fraudsters

strony usługi świadczone przez instytucje finansowe lub operatorów telekomunikacyjnych są przestępcom niezbędne do popełnienia przestępstw również z przyczyn czysto technicznych. Wykradzione środki trzeba przecież przelać na rachunek otwarty w jakimś banku, a oszukańczego SMS-a wysłać z numeru telefonu zarejestrowanego przez któregoś z operatorów telekomunikacyjnych.

To właśnie tego typu ponadnarodowe organizacje znajdują się obecnie na pierwszej linii frontu w walce z cyberprzestępczością. Mają one bowiem największe szanse na skuteczne przeciwdziałanie temu zjawisku, dzięki wykrywaniu podejrzanych zachowań jeszcze zanim dojdzie do popełnienia właściwego oszustwa. Predestynuje je do tego zarówno transgraniczny charakter prowadzonej działalności, umożliwiający skoordynowanie działań w wielu różnych jurysdykcjach, jak i wspomniana kluczowa rola ich infrastruktury w przeprowadzaniu niektórych rodzajów cyberprzestępstw.

Państwa coraz szczelniej oplatają tych przedsiębiorców różnorakimi regulacjami w celu zapewnienia bezpieczeństwa użytkownikom. To wszak zaufaniu użytkowników przedsiębiorcy zawdzięczają swój sukces gospodarczy. Są więc zobowiązywani do dbania o ich bezpieczeństwo tam, gdzie państwo nie sięga i nie byłoby wystarczająco sprawne. Jak jednak zawsze w tego typu przypadkach nie surowość regulacji, lecz ich egzekwowalność stanowi o ich skuteczności. Organy regulacyjne państwa nie dysponują wystarczającymi zasobami, aby zapewnić zgodność regulacyjną. Poszkodowani coraz częściej więc dochodzą roszczeń nie od sprawców – którzy pozostają nieuchwytni – lecz od „pośredników", którzy nie dołożyli wystarczającej staranności, aby przeciwdziałać przestępstwom popełnionym z wykorzystaniem ich infrastruktury.

Odpowiedzialność prawna jako zachęta do podjęcia działań

Duże międzynarodowe organizacje takie jak banki stosunkowo rzadko padają ofiarami cyberprzestępstw. Są bardziej świadome zagrożeń w cyberprzestrzeni i mogą ponieść o wiele większe nakłady niż przeciętne przedsiębiorstwo na zbudowanie odpowiednich zabezpieczeń. Poczuwają się również do odpowiedzialności za zapewnienie bezpieczeństwa informatycznego swoim klientom i zdeponowanym przez nich danym lub środkom finansowym. To poczucie odpowiedzialności o wiele rzadziej rozciąga się jednak na osoby trzecie, które stały się ofiarami oszustw popełnionych w oparciu o ich infrastrukturę czy renomę.

Co prawda stanowisko instytucji finansowych i innych instytucji zaufania publicznego w tym zakresie stopniowo się zmienia. Banki coraz częściej ostrzegają publicznie o różnego rodzaju oszustwach podszywających się pod serwisy bankowości elektronicznej (kampanie informacyjne banków ostrzegające o ryzyku *phishingu*), a niektórzy operatorzy telekomunikacyjni publikują

private enforcement to kluczowe narzędzie przeciwdziałania cyberprzestępczości

raporty na temat zagrożeń zidentyfikowanych przez ich wewnętrzne zespoły do spraw cyberbezpieczeństwa (np. raport CERT Orange Polska S.A.). Nadal nie można jednak mówić o działaniach mających na celu ogólną prewencję cyberprzestępczości popełnianej z wykorzystaniem ich infrastruktury. Jest to do pewnego stopnia zrozumiałe – na dostawcach usług krytycznych, w przeciwieństwie do organów władzy publicznej, nie spoczywa ogólny obowiązek przeciwdziałania przestępczości. Jako instytucje zaufania publicznego poruszają się jednak w rozbudowanej siatce regulacji przewidujących obowiązki publicznoprawne wiążące się do pewnego stopnia ze zwalczaniem cyberprzestępczości czy przestępczości w ogóle. Chodzi między innymi o ciążące na instytucjach finansowych obowiązki z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz zgłaszania wycieków danych osobowych lub danych objętych tajemnicą telekomunikacyjną. Od implementacji tzw. dyrektywy NIS doszedł do tego wyrażony wprost w ustawie obowiązek współdziałania z instytucjami publicznymi w ramach krajowego systemu cyberbezpieczeństwa.

Zakres stosowania się przez instytucje zaufania publicznego czy operatorów usług krytycznych do wspomnianych obowiązków w dużym stopniu zależy od egzekwowania zgodności regulacyjnej (*compliance*) przez poszczególnych regulatorów – Generalnego Inspektora Informacji Finansowej, Prezesa Urzędu Ochrony Danych Osobowych czy ministerstwa ds. cyfryzacji. Ich możliwości w tym zakresie często mogą być jednak ograniczone z uwagi na natłok obowiązków lub brak odpowiednich zasobów budżetowych czy kadrowych. Egzekwować zgodność z przepisami publicznoprawnymi mogą jednak również indywidualni uczestnicy obrotu prawnego. Chodzi o tzw. *private enforcement*, czyli możliwość wytoczenia powództwa wobec instytucji obowiązanej przez osobę poszkodowaną na skutek niedochowania obowiązków publicznoprawnych. W naszej ocenie jest to kluczowe narzędzie przeciwdziałania cyberprzestępczości, zwłaszcza oszustwom typu BEC i *phishingowi*, które pasożytują na infrastrukturze banków i operatorów telekomunikacyjnych. Ryzyko odpowiedzialności odszkodowawczej stanowi bowiem bardzo silny bodziec zapewniający należyte wykonywanie istotnych w tym zakresie obowiązków. Skuteczność tego mechanizmu dostrzegają zresztą sami ustawodawcy, w szczególności ustawodawca unijny. Możliwość wytaczania powództwa przez poszkodowanych naruszeniem obowiązków publicznoprawnych przewidują już wyraźnie przepisy unijne dotyczące prawa ochrony konkurencji, jak i przepisy dotyczące ochrony danych osobowych.

Private enforcement jako metoda zapobiegania cyberprzestępstwom

Znaczenie mechanizmu *private enforcement* dobrze widać na przykładzie przestępstw typu BEC. W uproszczeniu polegają one na tym, że oszuści przechwytują korespondencję (najczęściej mejlową) prowadzoną przez dwóch stałych kontrahentów, podszywając się pod jednego z nich. Z chwilą, gdy spodziewany jest stały przelew środków za określone usługi lub towary, przesyłają nieświadomej ofierze instrukcję, aby dokonała przelewu na inny niż zwykle rachunek bankowy. Rachunek jest przy tym pod kontrolą przestępców – został otwarty odpowiednio wcześniej za pośrednictwem tzw. słupa, który pozostaje w gotowości, aby wpłacone środki przekazać kolejnymi przelewami na rachunki bankowe otwarte w innych jurysdykcjach albo wypłacić je w gotówce i fizycznie przekazać mocodawcom. Stany Zjednoczone i Europa przeżyły istną falę tego typu przestępstw na przełomie 2014 i 2015 r. Są one bowiem stosunkowo łatwe do przeprowadzenia (choć wymagają znacznych przygotowań organizacyjnych), a możliwe do uzyskania zyski są dość wysokie. Pojedyncze przelewy mogą bowiem opiewać na kwoty do miliona dolarów lub euro, a przestępcy, którzy zorganizowali sprawnie działającą siatkę słupów, nie muszą przecież ograniczać się do jednej ofiary.

Kluczowym elementem w tego typu przestępstwach pozostaje bank. Oszuści muszą bowiem otworzyć rachunek bankowy, który będzie pod ich kontrolą i pozwoli wypłacić uzyskane środki pieniężne. W tym miejscu wkraczają do gry przepisy ustanawiające obowiązki w zakresie przeciwdziałania praniu pieniędzy. Jeśli bowiem banki z należytą starannością podchodzą do obowiązku identyfikacji i weryfikacji tożsamości nowego klienta, a także do wstępnej oceny ryzyka prania pieniędzy, bardzo często już na etapie zakładania rachunku mogą wychwycić, że nowy klient najprawdopodobniej działa jako tzw. słup i otwiera rachunek w podejrzanych celach, oraz zgłosić to odpowiednim instytucjom. Podobnie ma się rzecz z obowiązkiem bieżącego monitorowania transakcji pod kątem prania pieniędzy i wstrzymywania transakcji podejrzanych do czasu, gdy będzie mógł zadziałać organ odpowiedzialny za bezpieczeństwo finansowe w danym państwie.

Przy zachowaniu odpowiednich środków staranności przestępstwa typu BEC stają się o wiele trudniejsze do popełnienia. Falę tego typu cyberprzestępstw w dużym stopniu udało się zatrzymać właśnie z uwagi na wzmożoną ostrożność banków i innych instytucji finansowych. Ta wzmożona ostrożność wynikła jednak nie z ostrzeżeń publikowanych przez organy władzy publicznej, takie jak polski KNF czy FBI, ale z obaw o możliwość poniesienia odpowiedzialności odszkodowawczej wobec pokrzywdzonych. Od połowy 2015 r. sądy europejskie zaczęły bowiem wydawać orzeczenia, w których uznawały,

że banki mogą ponosić odpowiedzialność deliktową względem osób trzecich za szkody wynikłe z naruszenia obowiązków w zakresie przeciwdziałania praniu pieniędzy[2].

Podobne sprawy zostały również wszczęte przeciwko niektórym bankom w Polsce – nadal czekają jednak na rozstrzygnięcie, a treść przyszłych wyroków nie jest łatwa do przewidzenia. Kwestia możliwości pociągnięcia instytucji takiej jak bank do odpowiedzialności odszkodowawczej za naruszenie obowiązków publicznoprawnych, np. w zakresie przeciwdziałania praniu pieniędzy, ma bowiem charakter precedensowy i wiąże się z pewnymi istotnymi problemami prawnymi.

Przeszkody prawne dla *private enforcement* w Polsce i nowy paradygmat odpowiedzialności

Podstawową przeszkodą prawną do pociągnięcia banku lub innego rodzaju obowiązanej instytucji finansowej do odpowiedzialności deliktowej za naruszenie przepisów ustawy o przeciwdziałaniu praniu pieniędzy jest kwestia tego, jak należy rozumieć podstawową przesłankę bezprawności. Czy żeby uznać zachowanie banku za bezprawne wystarczy wykazać, że było ono sprzeczne z jakimkolwiek obowiązkiem (nakazem lub zakazem) ustanowionym przez powszechnie obowiązujące prawo? Czy też potrzeba czegoś więcej, tj. wykazania, że naruszony obowiązek miał właśnie na celu ochronę interesów dokładnie tych interesów majątkowych, które zostały na skutek jego niedochowania naruszone? Innymi słowy chodzi o pytanie, czy bank zachowuje się bezprawnie w każdym przypadku, gdy nie dochował obowiązków w zakresie przeciwdziałania praniu pieniędzy (o ile wynikła z tego szkoda dla kogoś), czy tylko jeżeli obowiązki te miały wyraźnie na celu chronić tę kategorię osób przed poniesieniem szkody.

Banki w postępowaniach prowadzonych w Polsce powołują się oczywiście na tę drugą koncepcję, wskazując, że przepisy o przeciwdziałaniu praniu pieniędzy nie mają na celu ochrony interesów indywidualnych uczestników obrotu, ale ochronę bezpieczeństwa systemu finansowego jako takiego. Koncepcja taka nosi w teorii prawa nazwę bezprawności względnej, a przeciwne rozwiązanie nazywa się bezprawnością bezwzględną. Istnieją pewne argumenty natury systemowej, które wskazują raczej na to, że polskiemu prawu deliktów bliższa jest koncepcja bezprawności względnej. W naszej ocenie kluczowe znaczenie dla rozstrzygnięcia tego problemu mają jednak przede wszystkim względy natury

2 Chodzi np. o wyrok Sądu Kasacyjnego w Luksemburgu z 26 marca 2015 r. (24/2015), a także wyrok Sądu Najwyższego w Holandii z 27 listopada 2015 r. (14/03217).

celowościowej. Z opisanych już wcześniej przyczyn wynika, że umożliwienie poszkodowanym cyberoszustwami możliwości dochodzenia odszkodowań od wykorzystanych w tym celu instytucji finansowych jest jedyną szansą na zwiększenie bezpieczeństwa zinformatyzowanego obrotu finansowego. To właśnie instytucje finansowe mają bowiem największe szanse na skuteczne przeciwdziałanie tego typu przestępstwom. Z uwagi na skalę prowadzonej działalności i postęp w zakresie jej cyfryzacji mają najlepszą wiedzę o aktualnych zagrożeniach i sposobach przeciwdziałania im. Ryzyko odpowiedzialności odszkodowawczej działa przy tym jako niezbędny bodziec do podjęcia odpowiednich kroków, zapewniających bezpieczeństwo także podmiotom trzecim, a nie jedynie im samym i ich klientom.

W sprawach dotyczących naruszenia przez banki obowiązków w zakresie przeciwdziałania praniu pieniędzy chodzi więc nie tyle o rozwiązanie teoretycznoprawnego problemu dotyczącego charakteru przesłanki bezprawności w prawie polskim, ile o zupełnie inne spojrzenie na rolę tego typu instytucji w kontekście współczesnej gospodarki cyfrowej. Sądy muszą rozstrzygnąć, czy w parze z ogromną skalą działalności banków i innych instytucji finansowych nie powinny iść równie daleko idące obowiązki o charakterze społecznym. Na razie pozostaje nam jedynie czekać na to rozstrzygnięcie. Niezależnie jednak od jego ostatecznej treści, wyroki wydane w tych sprawach z pewnością wpłyną również na zakres odpowiedzialności innych instytucji zaufania publicznego w innych obszarach prawa.

Jakub Barański
adwokat, praktyka postępowań sądowych i arbitrażowych

Łukasz Lasek
adwokat, praktyka postępowań sądowych i arbitrażowych oraz praktyka karna
solicitor Anglii i Walii (obecnie nie wykonuje zawodu)

instytucje finansowe mają największe szanse na skuteczne przeciwdziałanie cyberprzestępstwom

Sabina Famirska
Marcin Kulesza

Prawo ochrony konkurencji w dobie systemów AI oraz blockchaina

Technologie AI oraz blockchain tworzą nowe wyzwania w wielu obszarach prawa. Obydwa zjawiska są już widoczne także w sferze prawa ochrony konkurencji. Pierwsze, w kontekście algorytmów, zostało dostrzeżone w europejskiej i światowej praktyce, a drugie jest coraz istotniejszym przedmiotem rozważań.

e-commerce – algorytmy i zakazane porozumienia

Technologie AI w postaci algorytmów cenowych już od jakiegoś czasu pojawiają się w praktyce organów ochrony konkurencji i organizacji międzynarodowych.

W czerwcu 2017 r. OECD wydała opracowanie „Algorithms and Collusion: Competition Policy in the Digital Age", poświęcone analizie zagrożeń, jakie algorytmy niosą dla konkurencji. Jak zauważono, rozpowszechnione używanie algorytmów może, z jednej strony, nieść ze sobą korzyści dla przedsiębiorców i konsumentów, jednak z drugiej strony ich szeroko rozpowszechnione używanie może ułatwiać przedsiębiorcom zawieranie i utrzymywanie porozumień, zwłaszcza cenowych, bez żadnej formalnej umowy czy wręcz bez ingerencji ludzkiej.

W sierpniu 2016 r. Competition and Markets Authority, brytyjski ochrony konkurencji, wydał decyzję dotyczącą sklepów internetowych prowadzących działalność na platformie Amazon. Zgodnie z ustaleniami CMA, Trod Limited i GB eye Limited naruszyły zakaz porozumień ograniczających konkurencję, uzgadniając, że nie będą konkurowały cenowo („podcinały" swoich cen; CMA użyło frazy „*undercut each other's prices*"), sprzedając towary za pośrednictwem strony Amazon UK. Do monitoringu wykonywania tego porozumienia strony używały algorytmów cenowych. CMA nałożyła na Trod Limited karę

w wysokości 163 371 funtów; GB eye skorzystała z programu leniency i uniknęła kary.

W czerwcu 2018 r. luksemburski organ ochrony konkurencji wydał decyzję w sprawie Webtaxi, platformy rezerwacyjnej, która umożliwia rezerwację taksówki telefonicznie, przez internet lub za pośrednictwem aplikacji. W chwili złożenia zamówienia przez klienta platforma przypisywała mu najbliższą taksówkę oraz z góry, opierając się na ustalonych kryteriach obejmujących cenę za kilometr, dystans, warunki ruchu oraz opłatę początkową, określała cenę usługi. Cena nie podlegała negocjacji i wiązała klienta i kierowcę. Zdaniem luksemburskiego organu konkurencji system ten, choć stanowi ograniczające konkurencję porozumienie co do cen, nie naruszył konkurencji. Podkreślając korzyści, jakie niesie on dla klientów i przedsiębiorców (obniżenie cen przejazdów, krótszy czas oczekiwania na taksówkę przez klienta i na klienta przez kierowcę, mniej pustych przejazdów), a także zauważając, że system obejmował jedynie ok 26% rynku, a poza nim kierowcy nadal ze sobą konkurowali, organ uznał, że platforma ta może skorzystać z indywidualnego wyłączenia spod zakazu porozumień ograniczających konkurencję. Trzeba zauważyć, że decyzja ta jest przedmiotem dyskusji, a analiza korzyści przeprowadzona przez organ jest krytykowana.

Również w czerwcu 2018 r. rosyjski organ ochrony konkurencji nałożył karę na LG Electronics RUS. Organ podaje, że ukarana przezeń praktyka obejmowała ustalenie rekomendowanych cen odsprzedaży na rosyjskiej stronie internetowej LG, przekazanie informacji o tym fakcie odsprzedawcom, kontrolę stosowania przez odsprzedawców cen rekomendowanych oraz wymuszanie ich stosowania, w tym przez stosowanie sankcji (wstrzymywanie dostaw) za ich nieprzestrzeganie. Byłaby to klasyczna sprawa dotycząca wertykalnego ustalania cen odsprzedaży, gdyby nie fakt, że do monitorowania i kontrolowania stosowania cen rekomendowanych LG używał specjalnego oprogramowania opartego o algorytmy cenowe.

Wreszcie w lipcu 2018 r. Komisja Europejska, w czterech sprawach, których mechanizm był podobny do sprawy rosyjskiej, nałożyła kary wynoszące łącznie ponad 111 mln euro na producentów sprzętu elektronicznego domowego użytku (urządzeń kuchennych, komputerów przenośnych, sprzętu audio). Producenci ci ustalali ze sklepami internetowymi detaliczne ceny odsprzedaży swoich produktów i monitorowali wykonywanie porozumienia za pomocą specjalistycznego oprogramowania. Podobnie jak w sprawie LG, producenci sprzętu stosowali sankcje wobec niepodporządkowujących się detalistów.

Jak podkreśla Komisja Europejska, ograniczenie swobody cenowej dla określonych sprzedawców miało szerszy wpływ na rynek niż tylko w zakresie podmiotów objętych porozumieniem. Wpływ ten wynikał ze stosowania przez

większość sprzedawców internetowych oprogramowania opartego o algorytmy cenowe, które automatycznie dostosowuje ceny konkretnego sprzedawcy do cen konkurentów. Zatem podniesienie cen przez graczy objętych schematami skonstruowanymi przez producentów elektroniki wpływało na ceny także innych, konkurujących z nimi detalistów.

Warto zauważyć, że sprawy brytyjska i rosyjska zostały uwzględnione w analizie OECD.

Jak wynika z powyższych przykładów, algorytmy stosowane przez różne podmioty w procesie określania cen sprzedaży mają dwojaki wpływ na konkurencję. Z jednej strony, stanowią np. narzędzie wprowadzania i monitorowania ustaleń pomiędzy przedsiębiorcami zawierającymi porozumienie co do ograniczenia konkurencji cenowej. Trzeba przy tym zauważyć ryzyko związane ze stosowaniem algorytmów monitorujących ceny konkurentów, które mogą doprowadzić do stałej koordynacji cenowej, wyłączającej konkurencję i prowadzącej do podwyższenia cen.

Z drugiej strony, algorytmy i porównywarki używane w monitoringu cen konkurentów znacznie rozszerzają negatywne konsekwencje porozumień obejmujących jedynie część sprzedawców działających na rynku. Zwiększona w ten sposób szkodliwość wertykalnych porozumień cenowych, wychodząca znacznie poza krąg uczestników porozumienia, istotnie zwiększa tym samym ryzyko finansowe związane z karami antymonopolowymi nakładanymi na organizatorów i uczestników takich porozumień.

W obu aspektach zastosowanie algorytmów może rodzić lub zwiększać odpowiedzialność podmiotów zaangażowanych w praktyki cenowe ograniczające konkurencję.

Cenne w świetle powyższych przykładów podsumowanie zagrożeń związanych ze stosowaniem algorytmów cenowych przedstawił w lipcu 2018 r. Bundeskartellamt, niemiecki organ ochrony konkurencji. Zidentyfikowano cztery obszary ryzyka. Po pierwsze, w sektorach korzystających z analizy danych, np. w sprzedaży online, stosowanie algorytmów może prowadzić do zwiększenia przejrzystości rynku i umożliwiać bezpośrednie porozumienia cenowe poprzez automatyzację i rozszerzenie (jak w przypadku spraw europejskich) stosowania cen objętych porozumieniem. Po drugie, używanie algorytmów może stanowić samo w sobie porozumienie ograniczające konkurencję bez potrzeby bezpośrednich kontaktów między przedsiębiorcami. Po trzecie, algorytmy w systemach uczących się mogą same podejmować kluczowe decyzje, wykonywane automatycznie w systemach cenowych, które mogą ograniczać konkurencję. Po czwarte, używanie algorytmów może utrudniać wykrycie porozumień cenowych przez organy ochrony konkurencji, ich identyfikację oraz dowodzenie w sprawach porozumień ograniczających konkurencję.

Na tle tej analizy sformułowano daleko idące postulaty zmian w niemieckim prawie ochrony konkurencji. Zaproponowano wprowadzenie domniemania, że ograniczające konkurencję zastosowanie algorytmów cenowych prowadzi do zawyżenia cen, a także rozszerzenia odpowiedzialności za naruszenie zakazu porozumień ograniczających konkurencję na takie podmioty jak dostawcy usług informatycznych obejmujących algorytmy cenowe. Należy się spodziewać podobnych analiz i wniosków również w innych systemach prawnych.

Warto podkreślić, że temat sztucznej inteligencji jest obecnie przedmiotem szeroko zakrojonych prac Komisji Europejskiej. Komisja wraz z państwami członkowskimi do końca 2018 r. ma opracować skoordynowany plan działań w tej dziedzinie. Jednych z głównych elementów tych prac jest opracowanie kodeksu etyki dotyczącego rozwoju AI, który ma być zgodny z Kartą praw podstawowych Unii Europejskiej i uwzględniać tradycyjne zasady gwarantujące swobodną konkurencję, takie jak przejrzystość i dostępność danych. Zgodnie z zapowiedziami zasady etyczne mają dotyczyć m.in. transparentności algorytmów.

Blockchain i ryzyka związane z prawem ochrony konkurencji

Drugim istotnym wątkiem na styku nowych technologii i prawa ochrony konkurencji jest technologia blockchain. Technologia ta wciąż się rozwija, znajdując coraz szersze zastosowanie. Już obecnie zidentyfikowano jednak istotne ryzyka konkurencyjne związane z jej użyciem. Również tej kwestii swoje opracowanie poświeciła ostatnio OECD.

Istotnym elementem technologii blockchain jest przepływ i wymiana informacji. Zapisanie informacji w łańcuchu oznacza, że jest, a co najmniej może być ona dostępna dla każdego użytkownika. Transparentność informacji transakcyjnych obniża konkurencyjność rynku i może prowadzić do koordynacji między konkurentami, nawet do koordynacji czy ustalenia cen. Podobnie jak w przypadku algorytmów cenowych, blockchain może służyć do zawierania i monitorowania wykonywania porozumień ograniczających konkurencję.

Ściśle związana z technologią blockchain jest standaryzacja. Ustalanie nowych standardów na potrzeby kompatybilności platform musi uwzględniać ryzyka związane z potencjalnym ograniczeniem dostępu użytkowników do platform i do samego blockchaina. Standardy muszą zatem być transparentne, dostęp do platform i technologii musi być jednolity i niedyskryminacyjny. Różne platformy blockchaina powinny być względem siebie interoperacyjne i przez to zapewniać przejrzyste i łatwe interakcje między sobą.

Istotne w kontekście blockchaina jest ryzyko nadużycia pozycji dominującej. Technologia blockchain może stać się niezbędna do konkurowania

na określonym rynku (np. quasi-finansowym lub z wykorzystaniem smart kontraktów). Podmiot kontrolujący taką technologię może mieć wpływ na konkurencję na rynku. Ryzyko nadużycia może więc obejmować ograniczanie dostępu do technologii niezbędnej do prowadzenia działalności przez kontrahentów lub konkurentów. Możliwe jest także opóźnianie lub uniemożliwianie wprowadzenia lub rozwijania konkurencyjnych technologii blockchain przez podmiot dominujący na jakimś rynku związanym z tą technologią. Można sobie także wyobrazić sytuację, w której podmiot kontrolujący określoną platformę blockchain obniża koszty dostępu do niej w taki sposób, że można mu zarzucić tzw. drapieżnictwo cenowe prowadzące do odpływu użytkowników od konkurencyjnych platform, tym samym wykluczając je z rynku.

Wreszcie zawiązanie konsorcjum, którego przedmiotem lub narzędziem jest blockchain, może stanowić koncentrację w rozumieniu prawa ochrony konkurencji, rodzącą obowiązek zgłoszenia jej właściwemu organowi ochrony konkurencji odpowiedzialnemu za kontrolę koncentracji.

Jednym z najciekawszych tematów związanych z blockchainem jest możliwość wykorzystania tej technologii do rozwiązania problemów dotyczących trwałego nośnika. Zagadnienie stało się niedawno głośne w związku z decyzjami Prezesa Urzędu Ochrony Konkurencji i Konsumentów, który zakwestionował praktykę kilku banków, polegającą na udostępnianiu nowych regulaminów i tabeli opłat jedynie w wewnętrznym systemie e-bankowości. Tego rodzaju informacje należy przekazywać klientom banków na „trwałym nośniku". Za trwały nośnik uznaje się list w formie tradycyjnej lub elektronicznej, nośnik USB czy CD, oraz wiadomość email, o ile zawiera niezbędne dane. Udostępnianie w systemie e-bankowości nie spełnia kryteriów trwałości, ponieważ bank może dowolnie zmieniać treść wiadomości lub ją usunąć.

Takie zagrożenia może wyeliminować odpowiednio opracowana technologia blockchain, która zapisuje w formie rozproszonej całe dokumenty i nie pozwala na modyfikację ich treści. Obecnie możliwość zastosowania technologii w obrocie konsumenckim testuje jeden z wiodących banków w Polsce. Nie jest jeszcze znane stanowisko polskiego organu antymonopolowego w tej kwestii, ale wydaje się, że istnieją duże szanse na uznanie, że technologia blockchain pod pewnym warunkami może spełnić kryteria trwałego nośnika informacji.

Konsekwencje

Powyżej zidentyfikowano ryzyka naruszenia prawa ochrony konkurencji związane ze wszystkimi trzema zasadniczymi obszarami regulacji. Ryzyka zarówno w obszarze algorytmów cenowych, jak i w sferze blockchaina dotyczą porozumień ograniczających konkurencję, nadużycia pozycji dominującej i kontroli koncentracji.

Z każdym z tych ryzyk łączy się odpowiedzialność zaangażowanych w określoną działalność przedsiębiorców. W prawie polskim naruszenie prawa ochrony konkurencji w każdym ze wspomnianych obszarów wiąże się z potencjalną karą w wysokości do 10% obrotu przedsiębiorcy, nakładaną przez Prezesa UOKIK. Należy także mieć na względzie indywidualną odpowiedzialność osób zarządzających za zawarcie przez przedsiębiorcę porozumienia ograniczającego konkurencję.

Ryzyka te, tym wyższe, im mniejsza jest pewność co do stosowania prawa w tych obszarach, można minimalizować, dokonując szczegółowej analizy antymonopolowej przedsięwzięć wykorzystujących obie omawiane technologie. W szczególności należy pamiętać o prawie ochrony konkurencji w każdym przypadku koordynacji i współpracy – tak na polu oprogramowania opartego o algorytmy w procesie ustalania lub monitorowania cen, jak i w technologii opartej o blockchain.

Sabina Famirska
radca prawny, praktyka prawa konkurencji

Marcin Kulesza
praktyka prawa konkurencji

Krzysztof Wojdyło

Dane jako podstawowe aktywa nowej gospodarki

Globalna gospodarka w coraz większym stopniu jest oparta na danych. To one stają się podstawowym elementem napędzającym nowe modele biznesowe. System prawa nie jest na tę zmianę jeszcze gotowy. Od tego, jak prawo podejdzie do danych, zależeć będzie przyszłość gospodarki oraz jednostek.

Gospodarka oparta na danych

Widoczny wzrost znaczenia danych we współczesnej gospodarce jest wypadkową kilku czynników. Po pierwsze, wraz z postępującą cyfryzacją rzeczywistości nasz system społeczno-gospodarczy wytwarza coraz więcej danych. Po drugie, dysponujemy coraz lepszymi narzędziami do ich przetwarzania. Po trzecie, odkryliśmy olbrzymi potencjał tkwiący w danych. Ich odpowiednie przetworzenie daje istotną wartość dodaną, dostarcza nowej wiedzy o rzeczywistości, tworzy ciekawe modele biznesowe oraz buduje przewagę konkurencyjną. Po czwarte, dane stały się podstawowym zasobem niezbędnym do rozwoju systemów AI.

Doskonałą ilustracją potencjału, jaki niosą ze sobą dane, są modele biznesowe takich spółek jak Google lub Facebook. Dzięki dostępowi do ogromnej ilości danych o użytkownikach firmy te były w stanie stworzyć nowy model rynku usług reklamowych. Przetwarzanie danych o użytkownikach daje niespotykane wcześniej możliwości profilowania przekazu marketingowego. Uwolnienie potencjału związanego z danymi doprowadziło do rewolucji w branży marketingowej. A to tylko przykład jednego z wielu nowych modeli biznesowych, które mogą powstać w oparciu o dane.

Jakie prawo przysługuje do danych?

W obrocie gospodarczym pojawia się coraz więcej stosunków prawnych, których przedmiotem są dane. W języku potocznym zaczynamy posługiwać się takimi konstrukcjami jak „umowa sprzedaży danych", „wynajem danych" czy „użyczenie danych".

Tymczasem brakuje spójnej koncepcji rozumienia danych w systemie prawa. Istnieje szereg punktowych regulacji, które odnoszą się do wybranych aspektów prawnych danych. Bodaj najbardziej znanym i rozpoznawalnym przykładem są przepisy dotyczące danych osobowych. Często są one zresztą przywoływane jako jeden z podstawowych czynników ograniczających rozwój gospodarki opartej na danych. Regulacje te określają wiele istotnych aspektów dotyczących zasad przetwarzania danych. Odnoszą się jednak wyłącznie do danych osobowych. Ponadto nie rozstrzygają kluczowych zagadnień prawnocywilnych związanych z treścią ewentualnych uprawnień do danych.

Dane niewątpliwie stają się nowym aktywem. Jest to aktywo zasadniczo cyfrowe, które może być wykorzystywane wielokrotnie i nie podlega wyczerpaniu. Dane, o ile nie są przedmiotem zdefiniowanych przez system prawa praw własności intelektualnej, trafiają w prawną próżnię. Można sobie to łatwo wyobrazić, przywołując plastyczny przykład. Załóżmy, że mamy do czynienia ze startupem rozwijającym systemy AI. Systemy te są zasilane dużą ilością danych, które są gromadzone na serwerze spółki. Rynkowa wartość danych zebranych na serwerze przewyższa wielokrotnie wartość serwera. W wyniku egzekucji wyroku sądowego wydanego przeciwko startupowi wierzyciel spółki przejmuje własność serwera, na którym zapisane są wspomniane dane. Jakie uprawnienia i komu przysługują względem danych zapisanych na serwerze? Czy wierzyciel przejął na własność serwer, czy również zapisane na nim dane? Jeżeli tylko serwer, to jakie roszczenie ma względem wierzyciela startup? Jak może uzasadnić prawnie żądanie wydania danych, zakładając, że dane te nie obejmują danych osobowych?

Wiele z powyższych pytań pozostaje dzisiaj bez odpowiedzi, ponieważ system prawa nie definiuje treści uprawnień wobec danych. Nie mamy do czynienia z odpowiednikiem prawa własności wobec danych, które umożliwiałoby podmiotowi tego prawa skuteczne powoływanie się na jego uprawnienia względem każdego, kto to uprawnienie narusza. Mało tego, wśród prawników narasta spór wokół tego, czy takie prawo względem danych w ogóle powinno powstać.

Spór ten jest w dużej mierze spowodowany obawą przed tym, że wprowadzenie odpowiednika prawa własności w odniesieniu do danych może wytworzyć niebezpieczne ograniczenia w obrocie tymi danymi. Potencjał gospodarki opartej na danych będzie możliwy do wydobycia tylko wtedy, gdy zagwarantowany zostanie swobodny przepływ oraz możliwość przetwarzania tych danych. „Prawo własności danych" może stworzyć w tym kontekście trudne do pokonania przeszkody.

Z drugiej strony, uregulowanie prawnego statusu danych staje się pilną koniecznością w obliczu dynamicznego rozwoju relacji prawnych, których

przedmiotem są dane. Bez ustalenia cywilistycznego znaczenia prawa do danych obrót gospodarczy dokonywany w ramach nowej gospodarki będzie obarczony zbyt dużym ryzykiem.

Szerszy kontekst

Ustalenie prawnego statusu danych będzie zapewne wymagało interwencji ustawodawcy. Jakiekolwiek rozstrzygnięcie ustawodawcze w tym zakresie będzie musiało uwzględniać szerszy kontekst dyskutowanego zagadnienia. Otóż w dyskusji o prawnym statusie danych nie chodzi wyłącznie o wprowadzenie technicznego rozwiązania, które ułatwi obrót danymi. Chodzi również o ustalenie, jakie będą aksjologiczne fundamenty gospodarki opartej na danych.

Istota decyzji, którą będzie musiał podjąć ustawodawca, sprowadza się w dużej mierze do ustalenia roli jednostki w gospodarce opartej na danych. Jedną z naczelnych wartości systemu prawa europejskiego jest godność jednostki. Instytucje prawa europejskiego dążą do zapewnienia maksymalnej ochrony oraz realizacji tej godności.

Gospodarka oparta na danych stwarza tymczasem znaczące zagrożenia dla godności jednostki. Po pierwsze, tworzy ryzyko pozbawienia jednostki jej prywatności, która – przynajmniej do niedawna – była traktowana jako immanentny element ludzkiej godności. Po drugie, tworzy ryzyko pozbawienia jednostki godności w wymiarze ekonomicznym, poprzez swoiste uspołecznienie danych generowanych lub współgenerowanych przez jednostki.

Ryzyko w zakresie prywatności jest doskonale widoczne w przypadku znanych i popularnych serwisów internetowych, które budują swoje modele biznesowe w oparciu o dane użytkowników. Dostrzegamy naturalną tendencję do wymuszania przekazywania tym serwisom coraz większej ilości danych na temat zachowań i preferencji jednostek.

Ryzyko w wymiarze ekonomicznym sprowadza się do tego, że jednostki, mimo że w praktyce są wielokrotnie dostawcami surowca w postaci danych, nie partycypują w proporcjonalnym stopniu w korzyściach wynikających z wartości dodanej wygenerowanej przez przetworzenie tych danych. Dominujący w tej chwili model zakłada przekazywanie danych za darmo, w zamian za usługi dostarczane przez internetowych dostawców. Owszem, możemy korzystać z darmowych wyszukiwarek internetowych oraz mediów społecznościowych. Wiele wskazuje jednak na to, że wartość dostarczanych przez nas danych przewyższa wielokrotnie wartość dostarczanych nam w zamian świadczeń. Jest to o tyle istotne, że w obliczu postępujących procesów automatyzacji w gospodarce, które mogą skutkować ograniczeniem zatrudnienia, potrzebujemy pilnie alternatywnych sposobów generowania przychodu dla jednostek.

Dane są naturalnym surowcem, który w dobie cyfrowej rzeczywistości jest wytwarzany przez każdego z nas przez sam fakt funkcjonowania w przestrzeni społeczno-gospodarczej.

Ochrona godności jednostki w nowej gospodarczej ma swoją cenę. To spowolnienie rozwoju nowych modeli biznesowych, w tym w szczególności rozwiązań opartych na AI. Jurysdykcje, które zdecydują się chronić godność jednostki, będą musiały, przynajmniej krótkoterminowo, pogodzić się z utratą pozycji lidera w rozwoju nowej gospodarki.

Przedstawiony powyżej dylemat jest w praktyce zapewne znacznie bardziej zniuansowany, niemniej jednak jego istotą pozostaje wybór pomiędzy dążeniem do ochrony godności jednostki a efektywnością rozwoju nowej gospodarki. Rozstrzygnięcie tego dylematu dokona się w dużej mierze przy okazji rozstrzygania prawnego statusu danych. Bardzo ważne będzie w tym przypadku twórcze podejście, które – miejmy nadzieję – pozwoli znaleźć kompromisowe rozwiązanie, zapewniające ochronę godności jednostki przy jednoczesnym czerpaniu korzyści z gospodarki opartej na danych.

Krzysztof Wojdyło
adwokat, wspólnik odpowiedzialny za praktykę prawa nowych technologii

O kancelarii

Kancelaria Wardyński i Wspólnicy od 1988 roku jest trwale zakorzeniona w życiu prawniczym w Polsce. Skupiamy się na biznesowych potrzebach naszych klientów, pomagając im znaleźć skuteczne i praktyczne rozwiązanie najtrudniejszych problemów prawnych.

Dbamy o zachowanie najwyższych standardów prawniczych i biznesowych. Angażujemy się w budowę obywatelskiego państwa prawa. Bierzemy udział w projektach non profit i działaniach pro bono.

Nasi prawnicy są aktywnymi członkami polskich i międzynarodowych organizacji prawniczych, dzięki czemu mają dostęp do światowego know-how i rozwijają sieć kontaktów z najlepszymi prawnikami i kancelariami na świecie, z czego korzystają później nasi klienci.

Obecnie w firmie jest ponad 100 prawników świadczących obsługę prawną w języku polskim, angielskim, francuskim, niemieckim, hiszpańskim, włoskim, rosyjskim, czeskim i koreańskim. Nasze biura znajdują się w Warszawie, Krakowie, Poznaniu i Wrocławiu.

Dzielimy się wiedzą i doświadczeniem za pośrednictwem portalu dla prawników i przedsiębiorców (codozasady.pl), firmowego Rocznika, bloga prawa nowych technologii (newtech.law) oraz licznych seminariów, publikacji i opracowań.

wardynski.com.pl
codozasady.pl
newtech.law

Cykl publikacji na 30-lecie kancelarii Wardyński i Wspólnicy to zwięzłe, przekrojowe publikacje porządkujące i syntetyzujące nasze 30-letnie doświadczenia. Czerpiąc z tych doświadczeń, przedstawiamy wizje i rozwiązania na przyszłość.

Tom II poświęcamy innowacjom. Przypominamy nasz manifest, w którym wyjaśniamy, czemu prawnicy muszą zwiększyć zainteresowanie nowymi technologiami. Zastanawiamy się, czy – skoro wywalczyliśmy już sobie prawo dostępu do internetu – nie warto pomyśleć o prawie do wolności od internetu. Piszemy, co się zmieniło w wykonywaniu zawodu prawnika w ciągu 30 lat istnienia kancelarii. Wspominamy nasze pionierskie początki. Rozważamy wyzwania związane z autonomią systemów AI. Podpowiadamy, jak sobie poradzić z cyberprzestępczością (nie obejdzie się bez zaangażowania instytucji finansowych).

Wskazujemy, jaki wpływ sztuczna inteligencja oraz blockchain mają na prawo ochrony konkurencji. Przedstawiamy dylematy związane z podejściem prawa do danych w sytuacji, gdy są one podstawowymi aktywami nowej gospodarki, a wartość dostarczanych przez nas danych przewyższa wielokrotnie wartość otrzymywanych w zamian świadczeń.

30 lat WARDYŃSKI+ WSPÓLNICY