SZKOŁA DOKTORSKA UNIWERSYTETU SZCZECIŃSKIEGO
INSTYTUT NAUK PRAWNYCH

Marta Olga Grabowska
numer albumu: 2347

ROZPRAWA DOKTORSKA

Wpływ nowych technologii na funkcjonowanie zawodów prawniczych

Rozprawa doktorska napisana
pod kierownictwem promotora
dr hab. Aleksandry Monarchy-Matlak, prof. US

Szczecin 2023

Szczecin, dnia 27 lipca 2023 r.

OŚWIADCZENIE 1

Dotyczy: postępowania w sprawie nadania stopnia naukowego doktora na podstawie rozprawy pt. „Wpływ nowych technologii na funkcjonowanie zawodów prawniczych”.

Oświadczam, iż przedkładaną rozprawę doktorską napisałam samodzielnie. Oznacza to, że przy pisaniu pracy poza niezbędnymi konsultacjami nie korzystałam z pomocy innych osób, w szczególności nie zleciłam opracowania rozprawy lub jej części innym osobom, ani nie odpisałam tej rozprawy lub jej części z innych źródeł. Ponadto cytaty z obcych prac zostały wyczerpująco oznaczone oraz wskazane w przypisach i bibliografii mojej pracy. Przedkładana praca nie narusza przepisów ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (tekst jednolity Dz.U. z 2000 r., nr 80, poz. 904 z późn. zm.) również innych osób.

Jednocześnie przyjmuję do wiadomości, iż w przypadku nieprawdziwości powyższych oświadczeń, wszczęte zostanie postępowanie w sprawie uchylenia decyzji o nadaniu stopnia naukowego doktora.

……

Szczecin, dnia 27 lipca 2023 r.

OŚWIADCZENIE 2

Wyrażam zgodę na udostępnienie mojej rozprawy doktorskiej pt. „Wpływ nowych technologii na funkcjonowanie zawodów prawniczych”.

……

Spis treści

Wykaz skrótów

Akty prawne

Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.)

dyrektywa NIS – Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE. L.2016.194.1)

k.k. – ustawa z dnia 6 czerwca 1997 roku Kodeks karny (Dz. U. z 2023 r. poz. 289, 403, 818, 852)

k.p.a. – Ustawa z dnia 14 czerwca 1960 roku Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775)

k.p.k. – ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2023 r. poz. 289, 535, 818)

p.p.s.a. – ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2023 r. poz. 259, 803)

RODO – Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w s sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1)

Ustawa o informatyzacji – Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57, 1123, 1234)

Inne

AFIS – Automatyczny System Identyfikacji Daktyloskopijnej

AI – *Artificial intelligence* (Sztuczna Inteligencja)

BTS – *Base Transceiver Station*

CEPIK – Centrum Ewidencji Pojazdów i Kierowców

EKUZ – Europejska Karta Ubezpieczenia Zdrowotnego

e-PUAP – Elektroniczna Platforma Usług Administracji Publicznej

IP – *Internet Protocol Address*

KCIK – Krajowe Centrum Informacji Kryminalnych

KRK – Krajowy Rejestr Karny

KRS – Krajowy Rejestr Sądowy

KSIP – Krajowy System Informacyjny Policji

MSISDN – *Mobile Station International Subscriber Directory Number),* numer abonenta sieci komórkowej

NIP – Numer Identyfikacji Podatkowej

PESEL – Powszechny Elektroniczny System Ewidencji Ludności

PKB – Produkt Krajowy Brutto

SPP – System Poszukiwawczy Policji

SWP – System Wsparcia Prokuratora

UE – Unia Europejska

USA – Stany Zjednoczone

Wyrok TK – wyrok Trybunału Konstytucyjnego

Wyrok TSUE – wyrok Trybunału Sprawiedliwości Unii Europejskiej

Wstęp

W aktualnie otaczającej rzeczywistości nowe technologie mają bezpośredni wpływ na wszystkie dziedziny życia, na różnych jego płaszczyznach. Podążanie za rozwojem technologicznym sukcesywnie staje się jedną z najbardziej pożądanych wartości, a innowacyjne rozwiązania zaczynają być wykorzystywane przez zdecydowaną większość profesji. Z uwagi na nieustannie rosnące znaczenie nowych technologii i ich wykorzystanie, nie sposób dokonać zerojedynkowej oceny w tym zakresie, albowiem postęp technologiczny determinuje również ukształtowanie się zmian o negatywnych skutkach.

Nowe technologie odnoszą wpływ na zdecydowaną większość aspektów życia, w tym o charakterze społecznym, ekonomicznym i politycznym. W związku z tą tezą uznać należy, iż wpływ ten nie pozostaje również bez znaczenia w odniesieniu do bardzo szerokiej grupy zawodowej, jaką są zawody prawnicze. Dotychczas prowadzone badania naukowe w zakresie nowych technologii nie dostarczyły wyników badań pozwalających na podjęcie próby weryfikacji oceny stopnia tego wpływu jak również podjęcia próby wyodrębnienia jego następstw, zarówno o charakterze pozytywnym jak i negatywnym. Analiza wpływu nowych technologii na funkcjonowanie zawodów prawniczych stanowi aktualny i doniosły problem badawczy. Fakt udostępnienia coraz to nowszych, bardziej innowacyjnych i zaawansowanych rozwiązań w sposób zdecydowany ułatwia codzienne funkcjonowanie, z perspektywy społeczeństwa jako takiego, ale również w odniesieniu do jednostki.

Zawody prawnicze zdają się być niezwykle istotną branżą, zwłaszcza z punktu widzenia usług użyteczności publicznej, zaś z uwagi na coraz szerzej rozpowszechniane stanowisko w mediach w zakresie zagrożenia dla bytu tej grupy zawodowej w związku z rozwojem nowych technologii, w tym sztucznej inteligencji, kwestia ta stanowi ciekawy temat badawczy. Sposób wykorzystania nowych technologii w tej grupie zawodowej, fakt nadążania prawodawcy nad nieuchronnymi zmianami z perspektywy nowych technologii sprawia, iż przedmiotowe zagadnienia stały się punktem zainteresowania na tle niniejszej pracy. Rozwój nowych technologii generuje powstanie nowych sytuacji, w tym o charakterze prawnym, co z kolei implikuje konieczność wprowadzania nowych regulacji prawnych lub dokonania modyfikacji w przepisach już obowiązujących. Fakt ten następczo powoduje problemy prawodawcze w zakresie ewentualnego nadążania przez ustawodawcę w wprowadzaniu odpowiednich zmian na płaszczyźnie prawa powszechnie obowiązującego. Nie ulega również wątpliwości, iż nowe technologie i ich rozwój determinują kształt społeczeństwa informacyjnego, umożliwiając

scharakteryzowanie według bardziej zaawansowanych metod. Co więcej, postęp technologiczny powoduje pojawienie się zagrożeń, ale również coraz to nowszych wyzwań.

Przeprowadzenie kompleksowych, pełnych i rzetelnych badań w tym zakresie, opierających się przede wszystkim na aspektach praktycznych dotyczących zasadniczo organów ścigania, ale nie tylko, dostarczy wiedzy w zakresie faktycznego wpływu nowych technologii na funkcjonowanie zawodów prawniczych, zweryfikowania szans i zagrożeń z tym związanych, ale również podjęcia próby sformułowania postulatów pozwalających na maksymalne wykorzystanie potencjału nowych technologii w tej grupie zawodowej.

Niewątpliwie nowe technologie wywierają pozytywny wpływ na większość dziedzin życia społecznego, niemniej jednak, brak jest możliwości zerojedynkowej oceny, albowiem wyróżnić można również negatywne konsekwencje postępu technologicznego. W tym zakresie analizy wymaga kwestia cyberbezpieczeństwa oraz cyberprzestępczości, która w obliczu rzeczonych przeobrażeń staje się głównym nurtem przestępczych działań odnotowywanych na terenie kraju, a która stanowi jedną z negatywnych konsekwencji rozwoju technologicznego. Wykorzystanie nowych technologii przez sprawców przestępstw popełnianych za pośrednictwem sieci teleinformatycznej przybiera coraz to bardziej zaawansowany poziom, co bezpośrednio wpływa na możliwości wykrywcze organów ścigania. Odpowiedni dobór metod w tym zakresie, a także właściwe opracowanie algorytmu działania w procesie wykrywczym połączone z odpowiednio szybkim działaniem, zdaje się być interesującym tematem badawczym, wymagającym szczegółowej analizy, co w konsekwencji może stać się niejako szablonem w przypadku organizowania procesu mającego na celu zwalczanie i zapobieganie cyberprzestępczości.

Przedmiotowa praca ma na celu przybliżenie problematyki zagrożeń wynikających postępu technologicznego m.in. z punktu widzenia cyberbezpieczeństwa, ale również przytoczenie najbardziej kluczowych zagadnień związanych z potencjałem sztucznej inteligencji i jej faktycznym wykorzystaniem wśród profesji prawników, a nadto podjęcie próby oceny możliwości zastąpienia zawodów prawniczych przez algorytmy sztucznej inteligencji. Głównym celem rozprawy jest wykazanie stopnia wpływu nowych technologii na funkcjonowanie wszystkich zawodów prawniczych, a także ocena zaawansowania tego stopnia dokonana przez pryzmat szans i zagrożeń. Mając to na względzie, przedmiotowa rozprawa doktorska ma na celu przedstawienie zarówno pozytywnych jak i negatywnych następstw rozwoju technologicznego w odniesieniu do branży zawodów prawniczych, podjęcie analizy dotychczas obowiązujących rozwiązań prawnych w tym zakresie, a także sformułowanie

postulatów pozwalających na możliwie maksymalne wykorzystanie potencjału nowych technologii w tej grupie zawodowej, przy jednoczesnym poszanowaniu aktualnie obowiązujących przepisów prawnych w tym zakresie. W związku z tym, iż sztuczna inteligencja pozostaje w ścisłym związku z rozwojem technologicznym, na gruncie tej pracy, poddany zostanie również analizie problem badawczy bezpośrednio odnoszący się do wpływu sztucznej inteligencji na funkcjonowanie zawodów prawniczych, który aktualnie zdaje się być bardzo istotnym, z uwagi na popularyzacje stanowiska, zgodnie z którym byt zawodów prawniczych jest zagrożony przez sztuczną inteligencję.

Niniejsza praca powstała w odpowiedzi na szereg aktualnych i ważnych wyzwań pojawiających się w związku z nieustannym rozwojem technologicznym, rozpatrywanym w relacji do zawodów prawniczych, a głównie organów ścigania. Całość rozprawy została podzielona na sześć rozdziałów, wśród których dwa pierwsze mają w zasadzie charakter teoretyczny, niezbędny z punktu widzenia dalszych rozważań. Podjęcie próby definicyjnego opracowania pojęć, które będą regularnie używane na kanwie przedmiotowej rozprawy, a istotnych z perspektywy szeroko rozumianych nowych technologii, jest niezbędne w celu zapewnienia rzetelności i kompletności prowadzonych badań. Na gruncie rozważań podjętych w ramach przedmiotowej rozprawy analizie poddana zostanie siatka pojęciowa odnosząca się bezpośrednio i pośrednio do kwestii nowych technologii, a dotycząca komunikacji elektronicznej i jej środków, technologii informacyjno-komunikacyjnej (ITC), e-usług oraz technologii mobilnych, a także cyberprzestrzeni, cyberbezpieczeństwa i cyberprzestępczości. Przedstawienie kwestii teoretycznoprawnych związanych z funkcjonowaniem zawodów prawniczych ma natomiast na celu wskazanie zadań i kompetencji w odniesieniu do konkretnej grupy zawodowej, co w konsekwencji na tle późniejszych rozdziałów pozwoli na sformułowanie wniosków w zakresie rzeczywistego wpływu rozwiązań innowacyjnych na konkretną grupę zawodową w odniesieniu do określonej grupy zawodowej i realizowanych przez nią zadań.

W doktrynie nieustannie podnoszona jest kwestia dotycząca statusu polskiego społeczeństwa ocenianego przez pryzmat jego innowacyjności. Wskazania wymaga fakt, iż informacja sama w sobie stanowi aktualnie jedną z najbardziej pożądanych usług, a w obliczu nieustających zmian technologicznych, struktura i model społeczeństwa informacyjnego ulega sukcesywnym przeobrażeniom. W związku z brakiem w aktualnym dorobku naukowym wskazań dotyczących *stricte* statusu polskiego społeczeństwa jako społeczeństwa informacyjnego i społeczeństwa sieci, zwłaszcza po potężnych zmianach zaistniałych na skutek

pandemii koronawirusa w kraju i na świecie, podjęto próbę wyjaśnienia i przeanalizowania tej kwestii, a także przeprowadzenia badań ilościowych w tym zakresie. W związku z tym, w ramach trzeciego rozdziału przytoczone zostaną wyniki badań, pozwalające na ocenę grupy badawczej wykazującej się znacznym zróżnicowaniem, a w konsekwencji opracowanie satysfakcjonujących wniosków w tym zakresie.

Czwarty rozdział przedmiotowej pracy zdaje się być kulminacyjny z perspektywy zobrazowania wpływu nowych technologii na funkcjonowanie zawodów prawniczych i z wielu względów uznać można go za rozdział o charakterze wdrożeniowym. Rozdział ten stanowić będzie odpowiedź na najbardziej kluczowe problemy badawcze, związane przede wszystkim ze sposobem wykorzystania nowych technologii w konkretnych grupach zawodowych profesji prawniczych. Niemniej jednak zdecydowaną część czwartego rozdziału stanowią rozważania dotyczące nieprawdopodobnie negatywnego następstwa postępu technologicznego, wywierającego bezpośredni wpływ na cyberbezpieczeństwo a w konsekwencji pracę organów ścigania, których głównym zadaniem jest zwalczanie i zapobieganie przestępczości. Badania w tym zakresie przeprowadzone zostały w oparciu o praktyczny aspekt pracy tej grupy zawodowej. Na tle tego rozdziału szczegółowej analizie poddana zostanie kwestia cyberprzestępczości, niejako wprost wynikająca z nowych technologii, a także *modus operandi* sprawców oraz algorytm organów ścigania stanowiący odpowiedź na najliczniejszą grupę przestępstw popełnianych aktualnie na terenie kraju. Znaczący wpływ postępu technologicznego na działalność organów ścigania oraz wzrost popularności cyberprzestępstw coraz liczniej popełnianych na terenie kraju sprawia, iż badania w zakresie tej grupy zawodowej stanowią kluczowy problem badawczy. Działania realizowane przez organy ścigania, zwłaszcza prokuratorów, stanowią zespół powiązanych ze sobą czynności, bez wątpienia o niezwykle ciekawym charakterze, wymagającym odpowiedniego dostosowania do konkretnego stanu faktycznego. W ramach tych badań przeanalizowane zostaną typy i rodzaje cyberprzestępstw oraz scharakteryzowane zostaną przestępcze działania sprawców, a także oszacowana zostanie realna próba wykrycia przestępców w takich wypadkach. Rozwój technologiczny determinuje nieustannie kształtowanie się nowych sytuacji, w związku z czym w ostatniej części pracy sformułowane zostaną postulaty w odniesieniu do konkretnych grup zawodowych, które pozwolą w sposób maksymalny wykorzystać potencjał nowych technologii, przy jednoczesnym respektowaniu aktualnie obowiązujących przepisów prawnych.

W związku z rosnącym zainteresowaniem aspektami sztucznej inteligencji i jej potencjałem, a także coraz szerzej popularyzowanym stanowiskiem, zgodnie z którym stanowi ona zagrożenie dla bytu zawodów prawniczych, analizie poddane zostaną instrumenty i narzędzia oferowane przez sztuczną inteligencję, a także szanse i zagrożenia bezpośrednio wynikające z jej przyjmowania. Kompleksowe badania w tym zakresie pozwolą na sformułowanie wniosków w zakresie realnego zagrożenia dla tej grupy zawodowej, a także na oszacowanie ryzyka w tym zakresie, z bezpośrednim odniesieniem do określonej grupy zawodowej oraz konkretnych jej zadań.

Podjęcie możliwie kompleksowej analizy przywołanych problemów badawczych, niezwykle istotnych z perspektywy obecnie otaczającej rzeczywistości, w której na każdej płaszczyźnie dostrzegalne są przeobrażenia wynikające bezpośrednio z postępu technologicznego, pozwoli na sformułowanie wniosków doniosłych z perspektywy dorobku naukowego. Niewątpliwie nowe technologie dostarczają szeregu możliwości, również dla zawodów prawniczych, pozwalających na osiągnięcie bardziej satysfakcjonujących wyników pracy, przy jednoczesnym zminimalizowaniu czynnika czasu, który zwłaszcza w pracy organów ścigania staje się niekiedy najważniejszym aspektem. W związku z tym, na tle ostatniego z rozdziałów niniejszej pracy, sporządzone zostaną postulaty pozwalające na wykorzystanie maksymalnego potencjału jakie dostarczają rozwiązania innowacyjne wśród zawodów prawniczych, przy zachowaniu potencjału możliwości oferowanych przez aktualnie obowiązujący porządek prawny, a także zasygnalizowanie możliwości wprowadzenia niewielkich zmian legislacyjnych, które w ostatecznym wyniku mogłyby okazać się nieprawdopodobną szansą na sukces.

Mając na względzie powyższe, podstawowa teza przedmiotowej rozprawy doktorskiej sprowadza się do stwierdzenia, iż nowe technologie wywierają znaczący wpływ na funkcjonowanie zawodów prawniczych, powodując możliwość wyodrębnienia nie tylko pozytywnych, ale również, a w zasadzie przede wszystkim, negatywnych następstw rozpatrywanych z punktu widzenia cyberbezpieczeństwa. W związku z tym, jako tezę dodatkową wskazać należy również to, iż cyberprzestępstwa stanowią obecnie największą liczbę przestępstw popełnianych na terenie kraju, co bezpośrednio podyktowane jest rozwojem technologicznym oraz udostępnieniem dla potencjalnych sprawców przestępstw tego rodzaju, coraz to bardziej zaawansowanych narzędzi, pozwalających im na zachowanie pozornej anonimowości. Niewątpliwie sztuczna inteligencja wywiera istotny wpływ na funkcjonowanie omawianej grupy zawodowej, niemniej jednak realny stopień tego wpływu wymaga

dogłębnych badań w tym zakresie, odnoszących się bezpośrednio do instrumentów jakie oferuje sztuczna inteligencja, a następnie ich zestawienie z potencjałem prawników.

Przyjęte na tle niniejszej pracy metody badawcze obejmują przede wszystkim metody dogmatyczno-prawne, sprowadzając się do analizy aktów prawnych w powiązaniu z ugruntowaną w tym zakresie literaturą przedmiotu. Metoda ta uzupełniona została o metodę prawno-porównawczą oraz historyczno-prawną, a także *stricte* analizę praktycznych aspektów pracy organów ścigania, a zwłaszcza prokuratorów jako szczególnego rodzaju zawodu prawniczego. W związku z przyjętą metodą dogmatyczno-prawną, dokonano analizy przepisów obowiązujących w ramach porządku krajowego oraz międzynarodowego, w tym również unijnego, a także stanowiska doktryny. Metoda historyczno-prawna zapewniła możliwość wykazania zmian legislacyjnych przyjętych na przestrzeni ostatnich lat, ich uwarunkowania oraz konsekwencji.

Rozdział I

Istota nowych technologii

1. Analiza podstawowych pojęć

Dogłębna i szczegółowa analiza zastosowania szeroko rozumianej komunikacji elektronicznej wśród zawodów prawniczych wymaga w pierwszej kolejności wyjaśnienia, a następnie opisania kluczowych pojęć występujących w jej ramach. Wyłącznie kompleksowe omówienie zagadnień w tym zakresie, pozwoli na osiągniecie rzetelnych wyników badań. Posługiwanie się instrumentami komunikacji elektronicznej, sposobami jej wykorzystywania i regulowania przez prawodawcę, a w konsekwencji respektowania przez nią innych instytucji prawnych, minęłoby się w pełni z celem bez przeanalizowania kwestii pojęcia „komunikacji elektronicznej". Prawidłowe zdefiniowanie pojęć, które ze względu na specyfikę dziedziny, której dotyczą, są niejednokrotnie wysoce specjalistyczne, jest niezbędne z perspektywy możliwości podjęcia następczo badań o charakterze praktycznym i wdrożeniowym . Precyzyjna znajomość znaczenia pojęć, którymi się posłużono w niniejszej pracy, pozwoli z kolei na opracowanie pełnych i rzetelnych wniosków na podstawie kompleksowo przeprowadzonych badań.

Nowe technologie bez wątpienia oddziałują na wiele sfer życia społecznego, ekonomicznego oraz politycznego, począwszy od kwestii sądowych, administracyjnych oraz dotyczących bieżących czynności życia codziennego. W związku z tym, iż nowe technologie w aktualnej rzeczywistości odnoszą bezpośredni wpływ na wszystkie sektory gospodarki, jej wpływ nie pozostaje również bez znaczenia dla zawodów prawniczych i profesji występujących w tej grupie zawodowej.

1.1. Nowe technologie i konsekwencje ich rozwoju

W pierwszej kolejności możliwie najszerzej należy omówić i dogłębnie przeanalizować pojęcie nowych technologii, będących kluczowym zagadnieniem rozprawy. Wyjaśnienie kwestii zagadnienia zawodów prawniczych, w tym omówienie na czym polega ich funkcjonowanie należy na równi pod względem priorytetu traktować z zagadnieniem nowych technologii, niemniej jednak sfera ta jest na tyle obszerna i istotna, że wymaga przeanalizowania jej na kanwie odrębnego rozdziału, albowiem wykorzystanie nowych

technologii w przypadku poszczególnych zawodów prawniczych plasuje się i kształtuje zupełnie odmiennie, wykazując jednakże pewne zależności.

Nowe technologie stanowią obecnie jeden z najważniejszych elementów gospodarki. Rozwój w tym sektorze wpływa bezpośrednio na poprawę bytu i funkcjonowania niemal całego społeczeństwa. Niezwykle dynamiczny rozwój cywilizacyjny związany z postępem nowych technologii jednocześnie jest w stanie w sposób diametralny poprawić jakość życia człowieka, ale również doprowadzić do pojawienia się wielu zagrożeń zarówno dla jednostki jak i dla państwa[1]. Przykładem negatywnych konsekwencji rozwoju nowych technologii zwłaszcza z prawnego punktu widzenia, a pośrednio również z punktu widzenia organów ścigania są cyberprzestępstwa.

W pierwszej kolejności należy wyjaśnić genezę słów składających się na omawiane pojęcie. Słowo „technologia" pochodzi od greckich słów téchnẽ – sztuka, rzemiosło oraz lógos – słowo, nauka. Podejmując próby słownikowego wyjaśnienia tego pojęcia, należałoby wskazać, iż pojęcie „technologia" według takiej definicji oznacza przetwarzanie w sposób celowy i ekonomiczny dóbr naturalnych w dobra użyteczne (produkty), a także wiedzę o tym procesie[2]. W języku potocznym pojęcia tego używa się w znaczeniu innowacji, nowych środków techniki oraz wykorzystania ich w życiu codziennym[3]. Dla potrzeb przedmiotowych badań, niemniej jednak również w literaturze wskazuje się, iż w odniesieniu do technologii przymiotnika „nowe" oraz „nowoczesne" można używać w zasadzie zamiennie[4]. Definicja przywołanego pojęcia wielokrotnie pojawia się w wielu aktach normatywnych regulujących różne dziedziny prawa[5]. Przyjąć zatem można, iż nowe technologie są to innowacyjne rozwiązania, środki techniki umożliwiające komunikację, przetwarzanie oraz przekazywanie informacji, w różnych sferach życia społecznego i na wielu jego płaszczyznach. Mając na względzie znaczny wpływ rozwoju technologicznego na rozwój społeczeństwa na wielu płaszczyznach, jak również decydujący wpływ na proces zarządzania oraz przetwarzania i przesyłania informacji, uznać należy, iż odniesienie wyłącznie do dóbr niematerialnych jest znacznym ograniczeniem tej

[1] K. Chałubińska-Jentkiewicz , M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia,* Wolters Kluwer Polska, Warszawa 2015, s. 30 i nast.
[2] M. Szymczak., *Słownik języka polskiego*, t. 1–3, Państwowe Wydawnictwo Naukowe, Warszawa 1978–1981, s. 452
[3] K. Chałubińska-Jentkiewicz, *Rozwój nowoczesnych technologii w kontekście procesu stanowienia prawa na przykładzie strategii AI*, Teka Komisji Prawniczej PAN Oddział w Lublinie, t. XII, 2019, nr 2, s. 54
[4] Szerzej: B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), *Prawo sztucznej inteligencji i nowych technologii 2,* Wolters Kluwer, Warszawa 2022
[5] Np. art. 26c ust. 2 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. z 2023 r. poz. 28, 185, 326, 605, 641, 658, 825, 1059, 1114, 1130); por. A. Bartosiewicz, R. Kubacki PIT. Komentarz, wyd. V, Lex Wolters Kluwer Business, 2015

definicji. Świadomość wpływu dynamicznego postępu technologicznego na rozwiązania prawne jest w tym zakresie determinująca, albowiem implikuje stwierdzenie, iż definicja nowych technologii obejmuje również dobra materialne chociażby w postaci norm prawnych, ale również kwestie dotyczące rozwoju sztucznej inteligencji, nowej sieci komórkowej 5G i inne[6].

Mając na względzie poczynione wyżej ustalenia, możliwe jest sformułowanie definicji prawa nowych technologii, za które uważa się zespół norm prawnych, które odnoszą się do obszarów niezbędnej regulacji, w sferze relacji o charakterze zarówno publicznym, jak i prywatnym, na które bezpośredni wpływ wywierają nowoczesne technologie[7].

W odniesieniu do analizy definicyjnego ujęcia zakresu „nowych technologii" zasygnalizować należy, iż co prawda zdefiniowano to pojęcie na tle ustaw podatkowych, tj. ustawy z dnia 15 lutego 1992 roku o podatku dochodowym od osób prawnych[8] oraz ustawy o podatku dochodowym od osób fizycznych[9] (odpowiednio art. 18b ust. 2 oraz art. 26c ust. 2), niemniej jednak definicje te zostały stworzone wyłącznie dla celów przywołanych ustaw, zaś ich brzmienie niekoniecznie będzie wsparciem dla celów niniejszej pracy. Przyjąć można, iż nowoczesne technologie swoim zakresem obejmować mogą dobra niematerialne związane ściśle z zastosowaniem produktów będących efektem funkcjonowania nowych rozwiązań technicznych[10]. Podczas omawiania zjawiska nowych technologii nie sposób pominąć kwestii dotyczącej elementów występujących w związku z jego funkcjonowaniem, albowiem determinują one i umożliwiają prawidłowe funkcjonowanie szeroko rozumianej innowacyjności. Do tych elementów zaliczyć z pewnością należy oprogramowanie, usługi, bazy danych, wszelkie urządzenia elektroniczne umożliwiające przesyłanie oraz odbiór zbioru danych i informacji. W literaturze zgodnie podkreśla się, iż elementy te scharakteryzować można według wielu cech wspólnych, tj. globalny zasięg, szybkość, dynamiczność, przedsiębiorczość, konwergencja, partycypacja społeczna[11]. Niezwykle szerokie wykorzystanie nowych technologii zarówno w sferze politycznej i społecznej powoduje

---

[6] Szerzej: A. Kidyba (red.), A. Olejniczak (red.), *Nowoczesne technologie. Szansa czy zagrożenie dla funkcjonowania przedsiębiorców w obrocie prawnym i postępowaniach sądowych*, 2022

[7] K. Chałubińska-Jentkiewicz , M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia,* Wolters Kluwer Polska, Warszawa 2015, s. 21 i nast.

[8] Ustawa z dnia 15 lutego 1992 roku o podatku dochodowym od osób prawnych (Dz. U. z 2023 r. poz. 185, 326, 412, 825, 1059, 1130)

[9] Ustawa z dnia 26 lipca 1991 roku o podatku dochodowym od osób fizycznych (Dz. U. z 2023 r. poz. 28, 185, 326, 605, 641, 658, 825, 1059, 1114, 1130)

[10] K. Chałubińska-Jentkiewicz, *Rozwój nowoczesnych technologii w kontekście procesu stanowienia prawa na przykładzie strategii AI,* Teka Komisji Prawniczej PAN Oddział w Lublinie, t. XII, 2019, nr 2, s. 57 i nast.

[11] Ibidem.

przenikanie się obszarów regulacji prawnych, co w połączeniu z konwergencją prawną implikuje konieczność funkcjonowania szczegółowych uregulowań prawnych, które zdecydowanie powinny co najmniej nadążać nad postępem technologicznym. Oczywiście, nie jest zjawiskiem zaskakującym (i to w wielu krajach wysokorozwiniętych) to, że regulacje prawne nie pojawiają się równolegle wraz z rozwojem technologii, albowiem byłoby to irracjonalne, a nawet niemożliwe. Pojawianie się coraz to bardziej innowacyjnych środków, a następnie ich wykorzystywanie oraz podejmowanie działań w ich zakresie pozwala na zdefiniowanie i sformułowanie ewentualnych wątpliwości oraz zastrzeżeń, a w konsekwencji podjęcie rozwiązań prawnych ich niwelujących[12]. Najbardziej efektywnym i pożądanym zjawiskiem w tym zakresie jest możliwie najszybsza reakcja prawa na zmieniające się otoczenie i rzeczywistość, albowiem pozytywnie wpłynie to na prognozę wykorzystania tych środków, ale również na bezpieczeństwo i pewność obrotu prawnego. Zaznaczyć nadto należy, iż z uwagi na tempo rozwoju technologicznego system prawny musi być elastyczny, a wprowadzane rozwiązania muszą wykazywać się uniwersalnością, aby możliwe było wykorzystanie ich w skrajnie różnych przypadkach i zagadnieniach.

1.2. Technologie informacyjno-komunikacyjne (ITC)

Nie ma w zasadzie wątpliwości co do tego, iż aktualnie Internet w rozumieniu sieci teleinformatycznej jest nie tylko największym nośnikiem danych, ale również bez wątpienia najobszerniejszym zasobem informacji. Uprzednio głównym przekaźnikiem informacji był człowiek, następnie czasopisma i gazety. Po udostepnieniu nowych technologii zwłaszcza w postaci komputerów i telefonów istotnej zmianie uległ sposób przekazywania informacji, odnosząc bezpośredni wpływ m.in. również na relacje międzyludzkie. Aktualnie technologie te są obecne w niemalże wszystkich sferach życia, począwszy od pracy i nauki, skończywszy na rozrywce i życiu codziennym. Na przestrzeni lat znacząco wzrosły zasoby przetwarzanych danych, jak również szybkość ich przesyłania. W związku z wyżej przytoczonymi faktami w doktrynie wykształtowało się pojęcie społeczeństwa informacyjnego, które na przestrzeni lat było sukcesywnie udoskonalane i konkretyzowane[13]. Niemniej jednak materii tej zostanie poświęcona odrębna część niniejszej pracy z uwagi na złożoność i konieczność pełnej analizy tej kwestii.

[12] Por. P. Chmielnicki (red.), D. Mnich (red), *Prawo jako projekt przyszłości,* Wolters Kluwer, Warszawa 2022
[13] Szerzej: G. Szpor (red.), *Jawność i jej ograniczenia*, t. 1, *Idee i pojęcia*, Warszawa 2016, s. 114 i nast. oraz G. Szpor, A. Gryszczyńska *Internet. Strategie bezpieczeństwa*, Warszawa 2017

Istotne z punktu widzenia omawianych zagadnień jest również pojęcie technologii informacyjno-telekomunikacyjnych (ITC) lub inaczej technologii teleinformatycznych (z ang. *information and communication technologies*)[14], które odpowiadają za przesyłanie, gromadzenie, przetwarzanie i wizualizację danych w formie elektronicznej, są to wszelkie działania związane z produkcją i wykorzystaniem urządzeń telekomunikacyjnych i informatycznych oraz usług im towarzyszących[15]. Termin „technologie informacyjno-komunikacyjne", został po raz pierwszy użyty w 1997 r. w sprawozdaniu sporządzonym przez D. Stevensona dla rządu Wielkiej Brytanii i upowszechnił się w 2000 r. za sprawą dokumentów dotyczących nowego krajowego programu nauczania w tym kraju[16]. Węższym przedmiotowo pojęciem są technologie informatyczne (IT), które bezpośrednio dotyczą technologii związanych z komputerami i oprogramowaniem, niedotyczących jednak bezpośrednio technologii komunikacyjnych i sieci. Wszystkie działania związane z technologiami informacyjno-komunikacyjnymi odbywają się w ramach sektora ICT. Według definicji Polskiej Agencji Informacji i Inwestycji Zagranicznych (PAIZ) „sektor ICT to działania zajmujące się produkcją urządzeń komunikacyjnych i informatycznych oraz usługi im towarzyszące"[17]. PAIZ wyodrębnił siedem podstawowych branż w mniejszym lub większym stopniu powiązanych z ICT, dzieląc je na dwie grupy, tj. grupę produkcji urządzeń komunikacyjnych oraz grupę usług. Do pierwszej z wymienionych kategorii zaliczono sprzęt komputerowy, sprzęt komunikacyjny, sprzęt sieciowy i sprzęt do przesyłania danych, sprzęt biurowy. Natomiast w grupie usług znalazły się oprogramowanie, usługi telekomunikacyjne, usługi IT[18]. Narzędzia ICT można podzielić na cztery grupy umożliwiające analizę i syntezę informacji (przetwarzanie, selekcjonowanie, tworzenie spójnego obrazu z elementów umieszczonych w różnych obszarach); oddziaływanie, tworzenie, wykorzystywanie komunikatów medialnych (w tym multimedialnych), komunikację społeczną za pośrednictwem mediów informacyjnych, bezpieczeństwo systemów i danych[19]. Technologie informacyjno-komunikacyjne obejmują szeroki katalog technologii, w tym informacyjne,

[14] Szerzej: K. Chałubińska-Jentkiewicz , *Prawna ochrona treści cyfrowych,* Wolters Kluwer, 2021 oraz P. Pietrasz, *Informatyzacja polskiego postępowania przed sądami administracyjnymi a jego zasady ogólne*, Wolters Kluwer, 2020, s. 269 i nast.

[15] P. Pietrasz, *Konstytucyjne uwarunkowania informatyzacji postępowania przez sądami administracyjnymi,* Zeszyty Naukowe Sądownictwa Administracyjnego 2016/2/38-48

[16] R. Seweryn , *Technologie informacyjne i komunikacyjne*, C.H. Beck, Warszawa 2017, s. 14 i nast.

[17] https://www.istshare.eu/ict-technologie-informacyjno-komunikacyjne.html (dostęp: 10.03.2023 r.)

[18] Ibidem.

[19] W. Osmańska-Furmanek, M. Furmanek, *Technologie informacyjne cel czy narzędzie,* Chowanna 1, 132-149, 2006, s. 302–304

telekomunikacyjne, ale również nadawcze środki przekazu, różne rodzaje transmisji dźwięku i obrazu oraz kwestie dotyczące sieciowej kontroli i monitoringu.

1.3. Cyberprzestępczość

Jak wyżej wspomniano, rozwój nowych technologii wpływa na wiele sektorów gospodarki, na skutek czego możliwe jest wyodrębnienie nie tylko pozytywnych jego aspektów, ale również negatywnych konsekwencji. Pomimo, iż co do zasady rozwój w każdej dziedzinie odbierany jest z sympatią i wygląda obiecująco, to jednak nie zawsze możliwa jest jednoznaczna ocena w tym zakresie. Postęp technologiczny inicjuje coraz to skuteczniejsze rozwiązania i pomysły dla ewentualnych przestępców, niejednokrotnie zapewniając im anonimowość, co jest zdecydowanie bolączką organów ścigania[20]. Obecnie cyberprzestępczość, w tym oszustwa internetowe, wykorzystanie cudzych danych osobowych celem wyrządzenia szkody osobistej lub majątkowej, rozpowszechnianie treści pornograficznych, stanowi znaczną część generalnej liczby przestępstw popełnianych na terenie naszego kraju[21]. Szeroko rozumiana sieć telekomunikacyjna zdecydowanie ułatwia przestępne działania, pozwalając m.in. na zawarcie umów, zaciągnięcie zobowiązań przy wykorzystaniu wyłącznie Internetu, z jakiegokolwiek miejsca na ziemi.

Cyberprzestępczość, czyli najogólniej ujmując forma przestępczości polegająca na popełnianiu czynów zabronionych przy wykorzystaniu nowych technologii, zwłaszcza Internetu, w ostatniej dekadzie kilkukrotnie zwiększyła swoją częstotliwość[22]. Dostępność coraz to nowszych i przy okazji skuteczniejszych metod oraz dynamiczny rozwój narzędzi powoduje niemalże doskonałe ukrywanie się sprawców, a w konsekwencji nakłada na organy ścigania niebywale trudne zadanie jej zwalczania i wykrywania[23]. Niezwykle istotne w tym zakresie jest inicjowanie świadomości społeczeństwa w zakresie istniejących zagrożeń, co z pewnością może przyczynić się nie tylko do wykrywania sprawców, ale zwalczania tego zjawiska u źródła, zanim dojdzie do przestępnego działania. W nawiązaniu do wyżej wymienionych rodzajów cyberprzestępstw, które są aktualnie stanowią największą liczbę przestępstw popełnianych na terenie kraju, w związku z czym dominują w pracy organów ścigania, zwłaszcza na szczeblu rejonowym, wskazać należy, iż można je zakwalifikować do

[20] Szerzej: C. Banasiński, M. Rojszczak , *Cyberbezpieczeństwo,* Wolters Kluwer, Warszawa 2020
[21] K. Czaplicki (red.), A. Gryszczyńska (red.), G. Szpor (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Wolters Kluwer, 2019, s. 17
[22] https://www.ic3.gov/Home/AnnualReports?redirect=true (dostęp: 10.01.2023 r.)
[23] Szerzej: S. Alelyani , H. Kumar, *Overview of Cyberattack on Saudi Organizations*, „Journal of Information Security and Cybercrimes Research" 2018/1

różnych grup. Poniżej omówione zostaną podgrupy przestępstw popełnianych w cyberprzestrzeni, natomiast szczegółowy sposób działania sprawcy, w tym dokładne omówienie wykorzystanych przez niego metod oraz nowych technologii jak również wykorzystanie rozwiązań zapewniających mu anonimowość oraz możliwości organów ścigania w zakresie zwalczania tych przestępstw oraz wykrywania sprawców zostanie omówiona w kolejnym rozdziale.

Jednym z rodzajów cyberprzestępstw jest tzw. phishing – jest to rodzaj oszustwa polegającego na wyłudzeniu danych, np. numeru karty kredytowej wraz z kodem CVV lub dostępu do bankowości elektronicznej. Sprawca, w celu osiągnięcia korzyści majątkowej, zazwyczaj podszywa się (za pośrednictwem telefonu, adresu poczty elektronicznej lub strony internetowej) za jakąś instytucję, w tym bank[24]. Malware z kolei jest to swoistego rodzaju oprogramowanie, któremu należy przypisać przymiot złośliwego, albowiem jego zainstalowanie może doprowadzić do zainfekowania używanego urządzenia elektronicznego. Jego celem jest pozyskanie w sposób nielegalny różnego rodzaju danych, w tym również danych do logowania do bankowości elektronicznej[25]. Sprawca co do zasady przesyła „ofierze" adres strony internetowej, wprowadzając jednocześnie go w błąd co do rzeczywistego celu, po czym pokrzywdzony wchodząc w przesłaną stronę nieświadomie instaluje na swoim komputerze czy też smartfonie złośliwe oprogramowanie, które pozwala sprawcy na dokładne szpiegowanie swojej ofiary, uzyskując dostęp do wszystkich danych[26]. Do tego typu oprogramowania zaliczyć należy trojany, wirusy, oprogramowania szpiegujące (spyware, np. współcześnie najbardziej popularny i najbardziej skuteczny program AnyDesk) oraz randomware (blokujące dostęp do określonych zasobów lub systemu komputerowego)[27]. Nadto sposób działania sprawców pozwolił na wyodrębnienie przestępstwa Hackingu, czyli włamania, poprzez łamanie zabezpieczeń, umożliwiające zdalny, nielegalny dostęp do czyjegoś komputera oraz Cyberstalking czyli nękanie drugiej osoby przez Internet, poprzez wysyłanie niechcianych wiadomości w mediach społecznościowych, komunikatorach, pocztą elektroniczną. Innymi przykładami cyberprzestępstw są wszelkie oszustwa popełniane przez Internet, np. przez

[24] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Wolters Kluwer, 2020, s. 285 i nast.

[25] Por. R. Broadhurst , D. Lord, D. Maxim, H. Woodford-Smith, C. Johnston, H. Woon Chung , S. Caroll, H. Trivedi, B. Sabol , *Malware Trends on 'Darknet' Crypto-Markets: Research Review*, Australian National University Cybercrime Observatory 2018

[26] A. Kiedrowicz-Wywoał, *Pharming i jego penalizacja*, Prokuratura i Prawo 2011/6, s. 24–25

[27] *Do Web Hosts Protect Their Small Business Customers With Secure Hosting And Anti-Phishing Technologies? The Federal Trade Commission Staff Perspective*, https://cli.re/LqnQ7d (dostęp: 01.06.2023 r.)

nieuczciwych sprzedawców na portalach aukcyjnych, czy naruszanie praw autorskich (nielegalne kopiowanie i rozpowszechnianie filmów, muzyki) itp.

1.4. Cyberprzestrzeń i cyberbezpieczeństwo

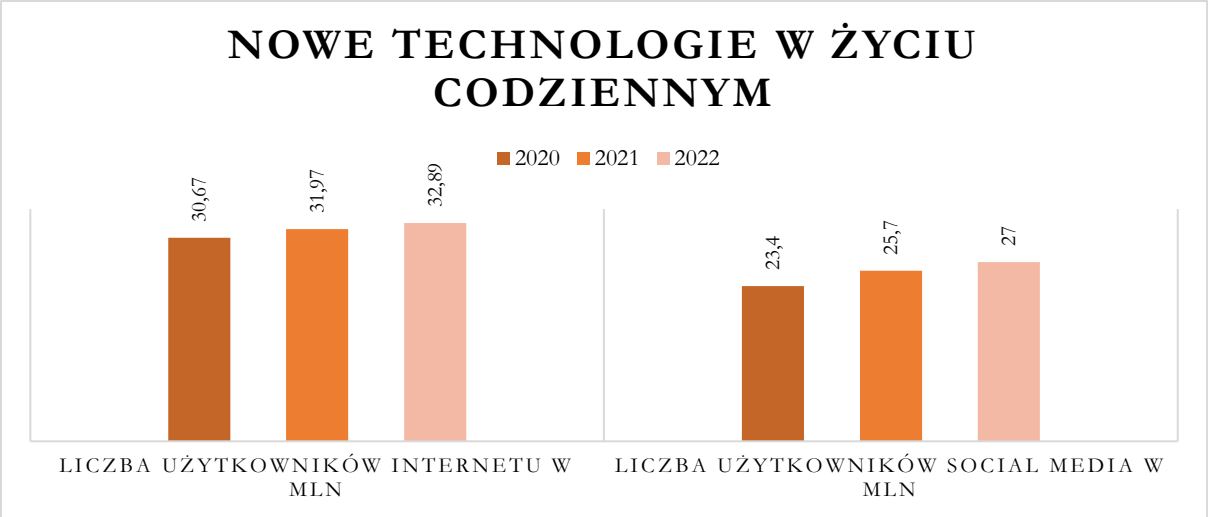
W zakresie omawiania nowych technologii nie sposób wspomnieć o cyberprzestrzeni. Jest to pojęcie stosunkowo nowe, co z uwagi na rozwijającą się dziedzinę prawa komunikacji elektronicznej, nie jest zaskakującym zjawiskiem. Pierwotnie pojęcie to używane było głównie w powieściach *science fiction*. Debata oraz analiza genezy tego pojęcia, pomimo braku definicji legalnej pozwala na wyodrębnienie pewnych jego cech – rozległość (zasięg światowy), spajanie wszelkich zasobów w jedną, olbrzymią bazę danych, złożoność oraz bezprzestrzenność rozumianą jako brak możliwości odniesienia cyberprzestrzeni do fizycznych (w tym geograficznych) wymiarów realnego świata[28]. Z uwagi na nieustannie rosnące znaczenie systemów teleinformatycznych oraz wykorzystanie ich na coraz większą skalę zainicjowało potrzebę stworzenia ustawowej definicji cyberprzestrzeni. W oficjalnym, elektronicznym słowniku pojęć z zakresu społeczeństwa informacyjnego można przeczytać następującą, zaproponowaną przez Komisję Europejską, definicję cyberprzestrzeni: Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata[29]. Poszukując definicji omawianego pojęcia w krajowym porządku prawnym wskazać w pierwszej kolejności należy, iż w dniu 2 listopada 2011 r. weszła w życie ustawa nowelizująca regulacje prawne stanów nadzwyczajnych. Implementując do polskiego porządku prawnego kwestię ochrony cyberprzestrzeni, wprowadzała również definicję omawianego pojęcia. Na podstawie założeń projektu Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011–2016 (dokumentu przyjętego ostatecznie w połowie 2013 r. pod nazwą Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[30] – o którym jest mowa dalej) wskazano, iż przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[31], wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[32]. Na tej podstawie uznać zatem należy, iż cyberprzestrzeń jest logicznie wyodrębnionym obszarem,

[28] Szerzej: J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Wolters Kluwer, 2020
[29] http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c (dostęp: 5.02.2023 r.)
[30] https://csirt.gov.pl/cer/publikacje/polityka-ochrony-cyber (dostęp: 5.02.2023 r.)
[31] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57, 1123, 1234)
[32] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego, 2013, s. 231

który ma charakter ponadnarodowy i tworzą go ściśle powiązane ze sobą systemy teleinformatyczne oraz występujące w jego ramach usługi i oprogramowania[33]. Oczywiście działanie w cyberprzestrzeni nie obejmuje wyłącznie wymiany informacji, albowiem cyberprzestrzeń „oferuje" wiele różnych usług i możliwości. Konsekwencją „bytu" cyberprzestrzeni jest obowiązek zapewnienia bezpieczeństwa działań podejmowanych w jej obszarze, co bezpośrednio implikuje konieczność naturalnego nadążania prawodawcy nad zmianami w dziedzinie technologii oraz konieczność przyjęcia uniwersalnych rozwiązań prawnych w tym zakresie.

Celem zobrazowania potężnego znaczenia, ale również wykorzystania nowych technologii w życiu codziennym warto wskazać kilka niezwykle szokujących liczb. Firma Hootsuite[34] zaprezentowała kolejną edycję raportu dotyczącego mediów społecznościowych na świecie oraz w poszczególnych krajach, wśród których znalazła się również Polska. Według raportu (stan na styczeń 2021 r.) z Internetu w Polsce korzysta 31,97 miliona osób, a więc 84,5% całkowitej populacji. W zakresie tym wykazano wzrost o 4,4%, tj. o 1,3 miliona użytkowników. Średni czas spędzony w Internecie przez użytkowników w wieku od 16 do 64 lat to 6 godzin i 44 minuty dziennie. Mediów społecznościowych używa 25,7 mln osób**,** a to zdecydowanie więcej niż połowa (68,5%) populacji naszego kraju (37,82 miliona osób). Porównując te dane z wynikami z 2020 r., wzrost wynosi aż 2,5 miliona (11%) w stosunku do roku poprzedniego[35]. W celu wykazania nieustannie rosnącej populacji Internetu w pełni uzasadnione jest przytoczenie danych według ww. raportu na styczeń 2022 r. Na początku 2022 r. w Polsce 87% całkowitej populacji korzystało regularnie z Internetu, co w odniesieniu do poprzedniego roku wykazuje wzrost o 2,5%. Aktualnie *social media* używane są przez 27 mln ludzi, a zatem przybyło 1,3 mln Polaków w zakresie aktywnych uczestników portali społecznościowych (72%)[36]. W zakresie średniego czasu spędzonego w Internecie, z raportu wynika pozytywny aspekt, albowiem jak się okazuje uległ on skróceniu o 5 minut i aktualnie wynosi 6 godzin i 39 minut dziennie, co bez wątpienia nadal jest bardzo wysokim wynikiem.

[33] G. Szpor (red.), *Jawność i jej ograniczenia*, t. 1, *Idee i pojęcia*, Warszawa 2016, s. 130 i nast.
[34] https://www.hootsuite.com (dostep: 2.03.2023 r.)
[35] https://www.econstor.eu/bitstream/10419/55888/1/687133424.pdf (dostęp 2.03.2023 r.)
[36] https://datareportal.com/reports/digital-2022-poland (dostęp: 2.03.2023 r.)



Wykres 1.

W celu pełnego zobrazowania wpływu postępu technologicznego na cyberprzestrzeń, oprócz dokładnej analizy wyżej wskazanych pojęć, badaniu poddać należy również kwestię cyberbezpieczeństwa[37]. Całokształt wyżej przytoczonych okoliczności w sposób bezpośredni wpływa na jego poziom[38]. Zgodnie z definicją legalną przyjętą w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[39], przez cyberbezpieczeństwo należy rozumieć odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Podstawy prawne cyberbezpieczeństwa zawarte w przepisach prawa powszechnie obowiązującego tworzy ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Ustawa ta wdraża do krajowego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE[40], zmieniając również niektóre przepisy w ustawy z dnia 7 września 1991 r. o systemie oświaty[41], ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[42] oraz ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[43]. Ustawa powiela materialne

[37] Szerzej: G. Szpor (red.), *Jawność i jej ograniczenia*, t. 1, *Idee i pojęcia*, Warszawa 2016, s. 130 i nast.
[38] T. Hoffmann, *Wybrane aspekty cyberbezpieczeństwa w Polsce*. Poznań 2018, Wydawnictwo FNCE, s. 16 i nast.
[39] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913)
[40] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (Dz. U. L 194 z 19.7.2016)
[41] Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz.U. z 2023 r. poz. 1234)
[42] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648, 1933, 2581)
[43] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r. poz. 122)

i proceduralne postanowienia dyrektywy NIS[44], dostosowując jednocześnie jej regulacje do warunków krajowych. Celem ustawy o krajowym systemie cyberbezpieczeństwa jest określenie organizacji oraz sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, jak i sposobu sprawowania nadzoru i kontroli w zakresie stosowania jej przepisów; uzupełniająco ustawa normuje także zakres i tryb stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej[45].

W świetle współczesnych realiów, gdzie dostęp do szybkich informacji i możliwość ich przetwarzania jest nie tylko gwarancją, ale również warunkiem sukcesu ekonomicznego, politycznego czy społecznego, nieustannie rosnąca cyberprzestępczość jest zjawiskiem naruszającym poczucie bezpieczeństwa i porządku publicznego[46]. Postęp technologiczny oraz kształtowanie się społeczeństwa informacyjnego doprowadziło do tego, że aktualnie bezpieczeństwo państwa jest ściśle powiązane z jego bezpieczeństwem informacyjnym. Bezpieczeństwo informacyjne określa potrzeby ochrony informacji. Przyjmuje się, że jest to zbiór działań metod i procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacjom lub zniszczeniem[47]. Od wielu lat dostrzegalny jest wzrost liczby cyberprzestępstw popełnianych na terenie kraju, które bezpośrednio ingerują w bezpieczeństwo przetwarzanych informacji. Pomimo wprowadzania nowych rozwiązań i środków trend ten pozostaje niezmienny. Wśród przyczyn tego zjawiska wskazuje się m.in. na brak jednolitych regulacji prawnych stwarzających narzędzia skierowane na wzmocnienie obszaru cyberbezpieczeństwa. Niezależnie jednak od powyższego bardzo istotne okazuje się zjawisko braku świadomości samych użytkowników sieci teleinformatycznej. Brak wystarczającej świadomości skutków podejmowanych działań w sieci uznawany jest za podstawę do realizacji przestępnego działania sprawców cyberprzestępstw. Żaden system cyberbezpieczeństwa nie będzie zatem kompletny bez odpowiedniego zbudowania aspektu świadomości jego użytkowników. Nie tylko administratorzy, ale również użytkownicy mogą podejmować szereg aktywnych działań ochronnych polegających na stosowaniu różnego rodzaju narzędzi i technik,

[44] Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE. L.2016.194.1)
[45] C. Banasiński, *Cyberbezpieczeństwo*. Zarys wykładu, Wolters Kluwer, Warszawa 2018, s. 16 i nast.
[46] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia,* Wolters Kluwer Polska, Warszawa 2015, s. 30 i nast.
[47] P. Potejko, *Bezpieczeństwo informacyjne,* Warszawa 2009, s. 194

w tym np. uwierzytelniania dwuskładnikowego polegającym na tzw. podwójnym zabezpieczeniu dostępu czy też szyfrowania danych przechowywanych na dysku lokalnym[48]. Tak współcześnie podstawowe narzędzia z pewnością w większym stopniu zapewnią bezpieczeństwo przechowywanych, przetwarzanych i przesyłanych danych, ale również zapobiegną popełnieniu w tym zakresie cyberprzestępstw[49]. Podkreślić należy, iż zastosowanie tych mechanizmów nie wymaga specjalistycznej wiedzy z zakresu IT, jak również nie wiąże się z dodatkowymi wydatkami.

Dla ujednolicenia siatki pojęciowej wykorzystywanych definicji wskazać należy, iż podstawowym elementem chroniącym sieć komputerową jest zapora sieciowa *firewall*, która jest sposobem zabezpieczenia sieci i systemów przed atakami mającymi na celu uzyskanie nieautoryzowanego dostępu do danych i zasobów chronionej sieci oraz pracujących w niej systemów[50]. Definicja ta odnosi się zarówno do sprzętu komputerowego, jak również jego oprogramowania – tzw. *firewall softwarowy*. Wyróżnia się trzy rodzaje zapór sieciowych. Pierwszym są zapory filtrujące, które – jak sama nazwa wskazuje – przepuszczają tyko te pakiety sieciowe, które są zgodne z regułami ustawionymi na danej zaporze. Kolejnym typem są translujące adresy sieciowe NAT (ang. *Network Adress Translation)* czyli ukrywające hosty wewnętrzne przed zewnętrznym monitorowaniem poprzez zmianę adresów IP tych hostów. Ostatnim rodzajem są tzw. zapory pośredniczące proxy, gdzie cała komunikacja na serwer http przechodzi przez proxy, które może filtrować ruch. Statystyka wskazuje, iż w odniesieniu do większości incydentów naruszających bezpieczeństwo w sieci nie jest prowadzone postępowanie karne, co bezpośrednio oznacza, iż w zdecydowanej większości przypadków osoby pokrzywdzone rezygnują z zainicjowania postępowania przygotowawczego, nie decydując się na zawiadomienie organów ścigania o popełnionych na ich szkodę przestępstwie.

1.5. Komunikacja

Komunikacja rozpatrywana w perspektywie nowych technologii stanowi istotne zagadnienie, wymagające jego precyzyjnego i kompletnego wyjaśnienia, przy czym w pierwszej kolejności celowe jest opisanie członów przedmiotowego terminu. Pojęcie komunikacja pochodzi od łacińskiego słów *communicare* i *communicatio* tzn. połączyć, uczynić wspólnym, przekazywać informacje, porozumiewać się, czyli dwukierunkowy

[48] C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo,* Wolters Kluwer, Warszawa 2020, s. 278 i nast.
[49] Szerzej: J. Kosiński, *Cyberprzestępczość* [w:] *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, 2013
[50] C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo,* Wolters Kluwer, Warszawa 2020, s. 278 i nast.

przepływ informacji oraz słowa *communio*, które oznacza – wspólność, poczucie łączności czyli wejście we wspólnotę[51]. Przyjąć należy, iż termin komunikacja jest wieloznaczny, albowiem w języku polskim może być on rozumiany i wykorzystywany na wiele sposobów. Komunikacja oznacza m.in. przekazywanie i odbieranie informacji w bezpośrednim kontakcie z drugą osobą, ale rozumiana może być również jako ruch środków lokomocji między odległymi od siebie miejscami; też: drogi, szlaki i środki lokomocji oraz przepływ informacji między urządzeniami, np. telefonami lub komputerami. Komunikacja opisywana jest również jako „łączność między oddalonymi od siebie miejscami za pomocą środków transportu, linii telefonicznych itp., przekazywanie wiadomości, porozumiewanie się"[52]. Komunikowanie się oznacza przede wszystkim przekazywanie informacji, zawiadamianie o czymś, a samo komunikowanie się znaczy tyle co utrzymywanie z kimś kontaktu, porozumiewanie się, udzielanie się otoczeniu[53]. Komunikacja może mieć charakter zarówno jedno- jak i obustronny, przy czym w pierwszym ze znaczeń jest po prostu przekazaniem informacji, natomiast w drugim – ich wymianą.

Nie ma w zasadzie wątpliwości co do tego, iż komunikowanie się jest procesem występującym między ludźmi. Nadto jest filarem i fundamentem życia społecznego, w sposób decydujący i oczywisty wpływającym na jego rozwój. Proces ten wykorzystywany był od zarania dziejów zarówno między obywatelami, jak również na szczeblu organów lokalnych jak i ogólnokrajowych. Komunikacja wraz z postępem ludzkości, jako pojęcie, również ewoluowała na przestrzeni dziejów. Pierwotnie sposobem komunikowania się były obrazki, ewentualnie proste pismo, które z biegiem czasu zaczęło przybierać coraz bardziej skuteczne postaci, w tym bezpośrednie rozmowy, które jednak poprzedzone zostały przekazywaniem za pośrednictwem osób trzecich, czyli tych których bezpośrednio nie dotyczył proces komunikacji, wieści i pogłosek. O ile metoda ta pozwoliła porozumiewać i komunikować się na odległość, o tyle uznać ją należy za dość zawodną, z uwagi na zbyt wiele „ogniw pośredniczących" pomiędzy nadawcą a odbiorcą komunikatu oraz zawodną pamięć ludzką[54]. Sposób komunikacji polegający na bezpośredniej wymianie informacji był, a w zasadzie wciąż jest jednym z najskuteczniejszych, z uwagi na jednoczesną obecność odbiorcy i adresata, co

[51] A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i w aktach prawnych*, Lingwistyka Stosowana 24:4/2017, s. 139–148
[52] A. Dmowska, *Podręczny słownik przysłów i powiedzeń*, Delta W-Z, 2004
[53] A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i w aktach prawnych,* Lingwistyka Stosowana 24:4/2017, s. 139–148
[54] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania,* Kraków 1999 r. Wydawnictwo Fundacji Postępu Telekomunikacji, s. 9 i nast.

zapobiega powstawaniu ewentualnych nieporozumień. Potrzeby ludzkości i doskonalenia dążyły do możliwości komunikowania się na odległość oraz w sposób usprawniający i ułatwiający komunikację, ale również zapewniający możliwość gromadzenia i ewentualnie ponownego odtworzenia przekazywanych informacji, co zainicjowało potrzebę utrwalania komunikatów w postaci pisma, na nośnikach różnego rodzaju, w zależności od możliwości i dostępu do surowców. W związku z potrzebą możliwego przyspieszenia komunikowania się, proces ten zaczął przybierać postać wymiany informacji na odległość. Co zrozumiałe, na początku wymiana informacji rozłożona była w czasie, albowiem ówczesne możliwości techniczne i komunikacyjne nie pozwalały na bezpośredni i natychmiastowy przepływ wiadomości. Obecnie natomiast, na skutek nieustannie postępującego postępu technologicznego, istnieje możliwość komunikowania się na odległość w wymiarze natychmiastowym. Technologia, w tym postać elektroniczna, umożliwia taki sposób komunikowania się.

1.6. Pojęcie informacji

Pojęcie informacji oraz danych pojawia się w różnych instytucjach prawnych, regulujących aspekty informatyzacji, komunikacji, w tym również elektronicznej. Art. 3 ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne[55] wielokrotnie posługuje się tym terminem, w związku z czym konieczne jest jego precyzyjne omówienie.

Nie sposób znaleźć uniwersalnej definicji terminu „informacja". W doktrynie przyjmuje się, iż informacja przekazywana obywatelowi to oświadczenie wiedzy podmiotu administracyjnego, dotyczące m.in. określonego stanu faktycznego lub prawnego oraz konsekwencji z tych stanów wynikających[56]. Nadto w zależności od potrzeb, ale również w zależności od typu nauki, w którym akurat wykorzystywane jest to pojęcie, definicja kształtowana jest na ich potrzeby i prezentuje się odmiennie, wykazując pewne podobieństwa. Informacja w podstawowym i ogólnym znaczeniu oznacza konstatację stanu rzeczy, wiadomość. Składa się ona ze znaków językowych, które tworzą logiczną całość, a w konsekwencji opisuje pewne zjawiska, obiekty, instytucje i inne stany rzeczy. Potocznie informację pojmuje się jako wiadomość. Informacja może być rozpatrywana w trzech

[55] Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57, 1123, 1234)
[56] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Business, 2008, s. 57

aspektach. Pierwszy, tj. syntaktyczny (dotyczy ilości informacji, jaka może być potencjalnie zawarta w danej wiadomości), semantyczny natomiast odnosi się do znaczenia i zawartości treściowej wiadomości, zaś pragmatyczny dotyczy przydatności informacji, tj. wartości informacji zawartej w wiadomości ze względu na realizowany przez odbiorcę cel. Nie są obecnie znane uniwersalne metody analizy informacji w znaczeniu semantycznym i pragmatycznym. W sensie syntaktycznym definiuje się informację albo poprzez ilość (miarę) informacji I (informacji teoria), albo jako synonim pojęcia dane[57]. Interdyscyplinarna analiza tego pojęcia, pozwala na przyjęcie, iż informacja co do zasady ma charakter niematerialny i jest przenaszalna, a nadto jest dobrem zmniejszającym niepewność[58]. Oprócz rzeczonych cech pozwalających określić specyfikację pojęcia informacja, wskazać należy również, iż informacja daje się łatwo rozprzestrzeniać, nadaje się do natychmiastowego przesłania, wprowadza porządek, jest podzielna i wspólna[59], tj. należąca do wszystkich lub wielu, a nadto zdecydowanie przyspiesza możliwość komunikowania się.

Zaznaczyć nadto należy, iż termin „dane" i „informacje" nie powinny być używane zamiennie. Już w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne dane są konsekwentnie odróżniane od informacji, co jest istotnym zabiegiem z punktu widzenia interpretacji aktów prawa nie tylko krajowego, ale również lub nawet przede wszystkim – unijnego, a nadto sprzyja poczuciu racjonalności prawodawcy. Przyjąć należy, iż dane opisują dany fakt za pomocą zbioru znaków o określonej formie i typie. Dopiero w momencie, kiedy zostanie im nadany określony kontekst i zostaną zinterpretowane, wówczas uznane mogą zostać za informacje. Niezbędne jest również określenie zależności pomiędzy terminem komunikacja a informacja. Oczywiście między tymi pojęciami istnieje silna i bezpośrednia zależność i związek, polegająca głównie na tym, iż informacja jest przedmiotem komunikacji i jej nośnikiem, zaś celem komunikowania się jest przekazywanie informacji, niezależnie od wybranej przez nadawcę metody. Szczególną odmianą komunikacji, która na tle niniejszej pracy jawi się jako konieczna do omówienia, decydująca, a w obliczu obecnych czasów kluczowa i najbardziej potrzeba to telekomunikacja. *Tele* – z grec. daleko, [60]*communicatio* – z łac. łączenie, zbliżanie, również ludzi. W najbardziej podstawowym

[57] Słownik PWN, https://sjp.pwn.pl (dostęp 10.11.2022 r.)
[58] G. Szpor [w:] U*stawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, Wolters Kluwer Business, s. 58; szerzej również: G. Szpor (red.), *Jawność i jej ograniczenia*, t. 1, *Idee i pojęcia*, Warszawa 2016, s. 98 i nast.
[59] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer business, 2008 s. 57
[60] R. Biskup, M. Ganczar, *Komunikacja elektroniczna w postępowaniu administracyjnym,* Państwo i Prawo 2008/1/59-71

znaczeniu przez telekomunikację należy rozumieć przesyłanie dźwięku i obrazu na odległość, ale również jest to dziedzina nauki i techniki oraz dział gospodarki zajmujące się tym zagadnieniem.

1.7. Komunikacja elektroniczna jako sposób komunikowania się

Powyżej omówione pojęcia dostarczają możliwości pełnego wyjaśnienia pojęcia komunikacji elektronicznej. W najbardziej szerokim rozumieniu przez komunikację elektroniczną należy rozumieć komunikowanie się, tj. przekazywanie określonych treści i informacji za pomocą urządzeń elektronicznych, zwłaszcza szeroko rozumianych urządzeń elektronicznych[61]. Uznać należy, iż właśnie ta forma przekazywania wiadomości przewyższa w niemalże każdym aspekcie wszelkie inne sposoby komunikacji, zwłaszcza z uwagi na szybkość, efektywność i natychmiastowość transferu wiadomości. Kolejnym argumentem przemawiającym na korzyść komunikacji elektronicznej jest możliwość nadania informacji z każdego miejsca z dostępem do komputera czy też innego urządzenia elektronicznego, niezależnie od strefy czasowej. Wadą przedmiotowego rozwiązania, która z drugiej strony odbierana może być jako pozytywna cecha, jest co do zasady konieczność odbioru przekazanej informacji również za pomocą urządzenia elektronicznego. Jak słusznie zauważa się w literaturze przedmiotowej komunikacja elektroniczna jest rezultatem złożonych i wielokrotnych operacji techniczno-fizycznych i formalno-logicznych. Przekazywana informacja w warstwie fizycznej – to bodziec, impuls, sygnał. W warstwie formalnej – to bit, znak, symbol; w warstwie semantycznej – to wiedza, świadomość, przekazywanie treści informacji do odbiorcy w formie zrozumiałej wiadomości[62].

W komunikacji musi istnieć porozumienie, tj. odbiorca musi wiedzieć i rozumieć intencję nadawcy, wówczas mamy do czynienia z komunikowaniem się. Jeśli adresat nie odczyta prawidłowo wiadomości od nadawcy, nie sposób mówić o komunikowaniu się. W przypadku natomiast komunikacji elektronicznej należy rozważyć kwestię momentu, w którym faktycznie mamy do czynienia ze skuteczna komunikacją. Nie ma wątpliwości w zasadzie, iż proces komunikowania się za pośrednictwem szeroko rozumianych komputerów rozpoczyna wprowadzenie danej informacji do wykorzystywanego aktualnie systemu, a następnie przesłanie go do jednego bądź większej ilości odbiorców, przy czym wybór należy do nadawcy

[61] Szerzej: A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Business, 2008

[62] A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i w aktach prawnych*, Lingwistyka Stosowana 24: 4/2017, s. 142

komunikatu. Jak wyżej wskazano, z komunikacją mamy do czynienia w momencie tzw. porozumienia i prawidłowego odczytania intencji inicjującego ten proces. W przypadku natomiast komunikacji szczególnego rodzaju, jakim jest komunikacja elektroniczna decydującym momentem jest odczytanie treści zawartej w komunikacie. Zasygnalizować jedynie należy, iż w zakresie komunikacji elektronicznej można wyodrębnić pewne jej rodzaje, które występują i funkcjonują w obrocie prawnym. Wyróżnić można komunikację elektroniczną internetową, czyli wykorzystującą łącza telekomunikacyjne, ciesząca się dużą popularnością oraz niemalże nieograniczonym charakterem i bezproblemową dostępnością. Natomiast komunikacja poza internetowa, wykorzystuje pozostałe sposoby komunikowania się za pomocą urządzeń elektronicznych.

1.8. Cechy komunikacji

Jak wyżej wskazano komunikacja jako pojęcie złożone oraz jako proces składający się z wielu ogniw, pozwala na wyodrębnienie cech ją charakteryzujących. Wśród nich wyróżnić można zindywidualizowany bądź grupowy charakter, wymóg świadomości po obu stronach, a nadto komunikacja posiada konkretny cel, wykorzystując przy tym zmysły. Cechą komunikacji jest również jej bezpośredni lub pośredni charakter[63]. W zakresie indywidualności komunikacji wskazać należy, iż informacja będąca jej nośnikiem może zostać zaadresowana do ściśle określonego podmiotu, konkretnej osoby, ale niejednokrotnie zdarza się również, iż dany komunikat kierowany jest do nieograniczonej grupy odbiorców. Proces przekazania informacji w drodze komunikacji elektronicznej, jak wyżej wskazano, nie jest skuteczny dopóty dopóki odbiorca nie zapozna się z informacją będącą treścią komunikatu. Czynność ta bez wątpienia wymaga istnienia świadomości po obu stronach procesu komunikowania się drogą elektroniczną, albowiem nadawca działa w ściśle określonym celu, natomiast odbiorca odbierając taką treść musi co najmniej zdawać sobie sprawę z intencji nadawcy.

Z uwagi na to, iż komunikacja elektroniczna jest szczególnym typem komunikowania z uwagi na wykorzystywanie podczas jej procesu szeroko rozumianych urządzeń elektronicznych, zwłaszcza komputerów wyodrębnić można pewne specyficzne jej cechy. Komunikacja elektroniczna charakteryzuje się natychmiastowością. Potrzeba możliwie najszybszego przekazywania komunikatów i informacji, ale również nieustanny postęp technologiczny zainicjował sposób komunikowania się w formie elektronicznej. Możliwość natychmiastowego przekazania treści, bez nakładu siły w postaci wysłania np. listu drogą

[63] J. Janowski, *Elektroniczny obrót prawny*, Seria Akademicka Prawo, Warszawa 2008, s. 152

tradycyjną z pewnością pozwala na uznanie tego sposobu komunikacji za najbardziej skuteczny. Komunikacja elektroniczna nadto wyposażona jest w cechę jednoczesności, pozwalającą niemalże w jednej chwili nadanie i odebranie komunikatu, co z pewnością wpływa na szybkość i pewność obrotu prawnego. Za pomocą komunikacji prowadzonej drogą elektroniczną umożliwiony nadto jest masowy przekaz, pozwalający na dotarcie do nieograniczonej liczby podmiotów – szeroko rozumianych. Cecha ta nadto pozwala na dotarcie do wielu podmiotów jednocześnie. Jako szczególną cechę komunikacji elektronicznej, wymagającą zdecydowanie jej wyodrębnienia i bardziej szczegółowego wyjaśnienia jest również konwergencja oznaczająca wielopłaszczyznowość oddziaływującą na różne zmysły[64]. W przypadku komunikacji niewykorzystującej urządzeń elektronicznych w przekazie informacji, co do zasady proces wygląda tak, że nadawca konstruuje treści, które następnie rekonstruowane są przez odbiorcę, wobec czego uznać należy, że sytuacja jest „mało skomplikowana". W przypadku komunikacji elektronicznej natomiast proces jest bardziej wymagający i złożony, albowiem składa się z procesów, które określić można jako techniczno-fizyczne oraz formalno-logistyczne. Mając na względzie wyżej poczynione rozważania, wskazać należy, iż urządzenia elektroniczne oraz rozwiązania technologiczne, za pomocą których dochodzi do komunikowania się są jedynie (albo aż) elementem procesu komunikowania się i bez wątpienia ułatwiają, a w zasadzie umożliwiają ten proces, natomiast komunikacja ewidentnie zachodzi pomiędzy ich użytkownikami.

Komunikacja elektroniczna obejmuje trzy odrębne dotychczas sektory: telekomunikację, technologie informacyjne i media elektroniczne. Obecnie komunikacja elektroniczna zatem obejmuje infrastrukturę komunikacyjną i związane z nią usługi świadczone za pośrednictwem szeroko rozumianych sieci teleinformatycznych, w tym Internetu, radiofonii, sieci satelitarnych i teleinformatycznych oraz sieci telewizji kablowej i inne. Jak wyżej wielokrotnie wskazano, komunikacja elektroniczna swoim zasięgiem obejmuje również urządzenia towarzyszące wyżej wymienionych usługom[65]. Z uwagi na szybko rozwijający się rynek urządzeń elektronicznych oraz nieustający postęp w tym zakresie, coraz częściej pojawiają się nowe urządzenia umożliwiające komunikację elektroniczną. W pierwotnym kształcie ten rodzaj komunikacji możliwy był wyłącznie przy użyciu komputera, obecnie

[64] A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i w aktach prawnych*, Lingwistyka Stosowana 24: 4/ 2017, s. 142

[65] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Business, 2008, s. 59 i nast.

jednak możliwy jest z wszelkich urządzeń z dostępem do szeroko rozumianej sieci[66]. W doktrynie wyróżnia się: rozmowę telefoniczną, w tym przy użyciu kamery rejestrującej jednocześnie obraz i dźwięk; wiadomości tekstowe, w tym SMS, mail; automatyczną wymianę danych, wykorzystującą np. ogólnoprzyjęte obrazki, tj. znaki twierdzące lub przeczące oraz kliknięcie odpowiedniego miejsca na ekranie urządzenia.

1.9. Wpływ rozwoju technologicznego na formy komunikacji elektronicznej

Współczesny świat jest idealnym obrazem nieustających przemian, które zauważalne są w każdej sferze. Nie sposób wytypować dziedziny, która z perspektywy minionych lat, nie przeszła totalnej rewolucji. W zależności od dziedziny oraz przedmiotu zmiany wyglądają zupełnie inaczej, natomiast bez wątpienia stwierdzić należy, iż postęp i rozwój jej zauważalny w każdej dziedzinie[67]. XX wiek zdecydowanie należy nazwać przełomowym z wielu powodów. Z pewnością był to decydujący moment w zakresie rozwoju technologicznego, a w konsekwencji przełom w naukach ścisłych. Wówczas znacznie zmieniła się świadomość społeczeństwa, ukształtowana przez ówczesne czasy, co bezpośrednio związane było z szeroko rozumianym dostępem do informacji. Przełom w tym zakresie powodujący wzrost znaczenia informacji oznacza, że informacja zaczęła odgrywać rolę decydującego czynnika produkcji[68]. Oznacza to, iż coraz więcej osób zostaje zatrudnionych w usługach związanych z dostarczaniem informacji. Chociaż wydawać by się mogło, iż w związku z rozwojem technologicznym, praca wielu ludzi może być zastąpiona czy też niepotrzebna, to jednak nic bardziej mylnego. Zrezygnowanie z jednego stanowiska pracy dostarczyć może ich nawet pięciokrotnie więcej. Nie ma podstaw, aby odmówić słuszności twierdzeniu, iż informacja stanowi obecnie jedną z najdroższych i najbardziej pożądanych dóbr.

Mając na względzie wyżej poczynione ustalenia związane z nieustannie rosnącą potrzebą dostępu do informacji, na przestrzeni lat zmieniały się sposoby i formy ich udostępniania, a rozwój technologiczny był idealnym środkiem wspierającym to zagadnienie[69]. Oczywiście cecha czasu była, i nadal jest, w tym zakresie kluczowa, albowiem potrzeba

[66] Szerzej: A. Monarcha-Matlak, *Wpływ komunikacji elektronicznej na prawo administracyjne* [w:] T. Bąkowski i in. *Prawo administracyjne dziś i jutro,* Wolters Kluwer, Warszawa 2018, s. 152 i nast.
[67] Szerzej: A. Kidyba (red.), A. Olejniczak (red.), *Nowoczesne technologie. Szansa czy zagrożenie dla funkcjonowania przedsiębiorców w obrocie prawnym i postępowaniach sądowych*, Wolters Kluwer, 2022
[68] M. Kuliński, *Regulacje Komunikacji Elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej,* CH Beck, Warszawa 2010, s. 5-11
[69] Szerzej: D. Skoczylas, *Aksjologiczny wymiar e-administracji i cyberbezpieczeństwa w kontekście potrzeb jednostki i wspólnoty* [w:] Z. Duniewska (red.), M. Karcz-Kaczmarek (red.), P. Wilczyński (red.), *Prawo administracyjne w służbie jednostki i wspólnoty,* Wolters Kluwer, Warszawa, 2022, s. 207 i nast.

możliwie najszybszego przekazu czy udostępnienia informacji jest nieodzownym elementem sprawnie funkcjonującego społeczeństwa oraz przyczynia się do pewności obrotu prawnego[70]. Nic zatem zaskakującego, iż „nowości" technologiczne niejednokrotnie wyprzedzają nowe formy udostępniania informacji, natomiast zarówno prawodawca krajowy, jak również europejski regularnie podejmuje próby nadążenia nad rozwojem oraz doskonalenia systemu komunikacji elektronicznej w sposób możliwie przybliżający kraje Unii Europejskiej do specjalistów na arenie światowej w tym zakresie[71].

2. Prawo komunikacji elektronicznej

Celem zapewnienia jasności i precyzji, a także zapewnienia bezpieczeństwa obrotu prawnego, konieczne jest ujęcie sfer omawianych na tle niniejszej pracy, w drodze odpowiednio przystosowanych aktów prawnych. Zaznaczyć należy, iż regulacje dotyczące komunikacji elektronicznej oraz dostępu do informacji znajdują się zarówno w prawie krajowym, jak również w prawie unijnym oraz regulacjach międzynarodowych.

2.1. Porządek krajowy

Poszukując regulacji prawnych dotyczących komunikacji, w tym również w wymiarze komunikacji elektronicznej, w pierwszej kolejności należy pochylić się nad Konstytucją RP[72]. Pierwsze uregulowanie odnoszące się do komunikacji i informacji prawodawca zawarł w art. 61 Konstytucji RP, zgodnie z którym każdy ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Dotyczy to również organów samorządu zawodowego i gospodarczego, a także innych jednostek organizacyjnych w zakresie, w jakim wykonują one działania władzy publicznej lub gospodarują majątkiem Skarbu Państwa, czy też mieniem komunalnym. Analiza przywołanego przepisu jednoznacznie wskazuje, iż powyższe prawo jednostki do informacji obejmuje dostęp do dokumentów, wstęp na posiedzenia organów kolegialnie wybranych, a nadto – co niezwykle istotne – możliwość jednoczesnej rejestracji dźwięku i obrazu[73].

Druga z regulacji, również określona przez prawodawcę w drodze Konstytucji RP dotyczy płaszczyzny regulującej uprawnienia państwa, a w konsekwencji organów władzy publicznej.

[70] Szerzej: P. Chmielnicki (red.), D. Mnich (red.), *Prawo jako projekt przyszłości*, Wolters Kluwer, Warszawa 2022
[71] Szerzej: K. Chałubińska-Jentkiewicz, *Prawna ochrona treści cyfrowych,* Wolters Kluwer, 2021
[72] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. z 1997 r. Nr 78, poz. 483, z 2001 r. Nr 28 poz. 319, z 2006 r. Nr 200, poz. 1471, z 2009 r. Nr 114, poz. 946)
[73] M. Florczak-Wątor [w:] P. Tuleja (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wyd. II*, 2021

Art. 51 Konstytucji niejako ogranicza swobodę władzy w tym zakresie, albowiem zgodnie z jego dyspozycją obowiązek ujawnienia informacji może zostać nałożony wyłącznie w drodze ustawy. Ustęp 2 konsekwentnie ogranicza uprawnienia państwa w tym zakresie, stanowiąc, iż pozyskiwanie, gromadzenie i udostępnianie informacji dotyczących obywateli jest możliwe i dozwolone wyłącznie w zakresie w jakim jest to niezbędne z punktu widzenia zasad demokratycznego państwa prawa. Powyżej przywołane regulacje bez wątpienia wywodzą i opierają się na jednej podstawie aksjologicznej, która z jednej strony przyznaje bardzo szerokie uprawnienie w zakresie dostępu do informacji, swobody komunikowania się, ograniczając jednocześnie swobodę państwa w zakresie ich rozpowszechniania[74].

Powyżej przytoczone regulacje, z uwagi rangę aktu prawnego, w jakim się znajdują zostały wspomniane jako pierwsze. Nie budzi wątpliwości natomiast celowość uregulowania kwestii dotyczących informacji oraz zagadnień z nią związanych – w drodze ustawowej. W porządku krajowym znajduje się szereg ustaw oraz wydawanych na podstawie ustawowych upoważnień aktów wykonawczych w postaci rozporządzeń. Sfera komunikacji elektronicznej, dostępu do informacji, ale także ich gromadzenia, przechowywania jak również stricte środków komunikacji elektronicznej poruszona jest na tle różnych ustaw, w tym m.in. ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne, ale również w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[75] a nadto w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[76]. Nie sposób jednak na tle niniejszej pracy omówić wszystkich ustaw regulujących omawianą dziedzinę, a tym bardziej dyspozycji w nich zamieszczonych.

Nie ma wątpliwości co do tego, iż sukcesywne wdrażanie technologii informacyjno-komunikacyjnych jako narzędzi komunikacji elektronicznej[77] wywiera bezpośredni wpływ na konieczność modyfikacji nie tylko w przepisach prawa administracyjnego, ale również w strukturach państwa, oddziaływania państwa na obywatela oraz sposobach jego funkcjonowania. Technologie komunikacyjne, zwłaszcza elektroniczne modernizują sposób funkcjonowania państwa, a społeczeństwo informacyjne osiąga inny wymiar, który być może doprowadzi do zmiany jego statusu na społeczeństwo cyfrowe, albowiem dzięki rozwojowi technologicznemu dostęp do informacji i usług jest zdecydowanie łatwiejszy, a zarządzanie

[74] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Business, 2008, s. 43
[75] Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. z 2023 r. poz. 756, 1030)
[76] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902)
[77] A. Monarcha-Matlak, *Prawo administracyjne dziś i jutro*, red. J. Jagielski, M. Wierzbowski, Wolters Kluwer, 2018, s. 152

danymi oraz usługami staje się standardem dla społeczeństwa. Mając na względzie powyższe w porządku krajowym pojawiła się również kwestia potrzeby uregulowania szeroko rozumianych aspektów związanych z prawem komunikacji elektronicznej, który obecnie znajduje się w fazie projektu ustawy Prawo komunikacji elektronicznej, w wersji z dnia 15 lutego 2021 r., opracowany został przez Ministra Cyfryzacji. Inicjatywa tego projektu bezpośrednio wynika z dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Oprócz dyrektywy 2018/1972[78] projekt wdraża też w prawie polskim trzy inne unijne akty prawne, przy czym o ile te trzy dyrektywy obowiązują w Unii Europejskiej już od wielu lat, w związku z czym również w Polsce były od dawna implementowane, o tyle dyrektywa 2018/1972 jest na arenie Unii Europejskiej stosunkowo nowym aktem prawnym, który miał być wdrożony przez państwa członkowskie UE do dnia 21 grudnia 2020 r. Celem projektu jest m.in. wdrożenie rynku wewnętrznego w dziedzinie sieci i usług łączności elektronicznej prowadzące do realizacji i rozpowszechniania sieci o bardzo dużej przepustowości, powstania zrównoważonej konkurencji, interoperacyjności usług łączności elektronicznej, dostępności, bezpieczeństwa sieci i usług oraz korzyści dla użytkownika końcowego, zapewnienie świadczenia w całej Unii Europejskiej publicznie dostępnych, przystępnych cenowo usług dobrej jakości poprzez skuteczną konkurencję i wybór, tak aby sprostać sytuacjom, w których rynek nie zaspokaja w sposób zadowalający potrzeb użytkowników końcowych oraz ustanowić niezbędne prawa użytkowników końcowych. Pozytywnie należy ocenić ruch prawodawczy w tym zakresie, albowiem ewentualna zmiana Prawa telekomunikacyjnego byłaby zbyt pracochłonna, wprowadziła trudności przy interpretacji, zwłaszcza mając na względzie potrzebę zmodyfikowania, ujednolicenia, uporządkowania oraz uproszczenia tych przepisów.

Projekt ustawy Prawo komunikacji elektronicznej został sporządzony przez Ministerstwo Cyfryzacji i został opatrzony datą 29 lipca 2020 r.[79]. Projektowana ustawa ma na celu zastąpienie aktualnie obowiązującej ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne. Prawie dwadzieścia lat, które minęło od uchwalenia rzeczonej ustawy, to w przypadku rozwoju technologii cała wieczność. Przez ten okres postęp technologiczny jest nieprawdopodobnie dostrzegalny, wiele aspektów dotyczących tej sfery usług przeszło całkowitą modernizację, sukcesywnie są udostępniane coraz to bardziej innowacyjne metody i narzędzia umożliwiające

[78] Dyrektywa Parlamentu Europejskiego i Rady UE 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz. U. UE L 321/36)

[79] https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?id=66C7F7C637867159C12589170035C136 (dostęp: 31.03.2023 r.)

szeroko rozumianą komunikację elektroniczną, w związku z czym nie ma żadnych wątpliwości co do konieczności natychmiastowego wprowadzenia zmian w regulacjach prawnych[80]. Mając na względzie przytoczone okoliczności, jednoznacznie wskazać należy, iż ustawodawca powinien niezwłocznie zareagować na dynamiczne zmieniającą się sytuację w celu dostosowania regulacji prawnych w zakresie nowych technologii do aktualnie obowiązujących warunków i sytuacji na rynku, uwzględniając zwłaszcza fakt sukcesywnego przyjmowania nowelizacji prawnych na szczeblu Unii Europejskiej. Za wprowadzeniem nowej regulacji przemawiać ma również zakres i liczba zmian, które nastąpiły w przepisach we wspomnianym okresie, co powoduje konieczność uporządkowania przepisów z zakresu prawa telekomunikacyjnego. Projektowane przepisy mają w zamiarze zastąpić ustawę Prawo telekomunikacyjne, które obecnie szczegółowo reguluje aspekty związane z działalnością telekomunikacyjną. Niemniej jednak, jak wynika z projektu ustawy, zakres przedmiotowy Prawa Komunikacji Elektronicznej będzie jeszcze szerszy, albowiem obejmie nie tylko tradycyjny sektor usług telekomunikacyjnych, ale również zagadnienia związane z usługami OTT (Over-the-top), tj. komunikacją interpersonalną, która odbywa się bez wykorzystania numerów (np. poprzez komunikatory takie jak Messenger, Skype czy WhatsApp), które obecnie znane jako tzw. usługi hybrydowe są jednym z najbardziej popularnych sposobów komunikacji elektronicznej.

2.2. Prawo unijne

Nie ulega wątpliwości, iż nie tylko prawo krajowe reguluje sferę dotyczącą prawa komunikacji elektronicznej. W obrocie prawnym mamy do czynienia z coraz to większą ilością decyzji podejmowanych na szczeblu europejskim. Organy Unii Europejskiej w tym zakresie wydają szereg rozwiązań, sprzyjających porządkowaniu, harmonizacji oraz rozwoju prawa komunikacji elektronicznej. Kluczowe i niezwykle istotne w tym zakresie jest rozporządzenie regulujące kwestię ochrony danych osobowych, które z punktu widzenia przekazywania informacji drogą elektroniczną – jest niezwykle ważne i potrzebne, aby zapewnić bezpieczeństwo obrotu prawnego[81]. Dynamicznie rozwijająca się sfera komunikacji wymaga zmiany podejścia oraz przede wszystkim zmiany uregulowań na wielu płaszczyznach, w tym prawnej, ekonomicznej, społecznej oraz politycznej. Decyzje podejmowane w tym zakresie na

[80] A. Monarcha-Matlak, *Komunikacja elektroniczna, prawo komunikacji elektronicznej, Europejski kodeks łączności elektronicznej i ich wpływ na rozwój jurysdykcji administracyjnej* [w:] M. Kruś (red.), L. Staniszewska (red.), M. Szewczyk (red.) *Kierunki rozwoju jurysdykcji administracyjnej*, Wolters Kluwer, Warszawa 2022, s. 267 i nast.

[81] Szerzej: W. Gromski i in., *Europejskie i polskie prawo telekomunikacyjne,* LexisNexis 2004

szczeblu europejskim w konsekwencji bezpośrednio pociągają za sobą konieczność uregulowania tych kwestii w porządku prawnym. Na tle niniejszej pracy zostanie zbadana kwestia nurtującego zagadnienia dotyczącego tego, czy prawodawca (zarówno krajowy jak i unijny) nadąża nad postępem technologicznym.

Nie ma wątpliwości co do tego, iż uregulowania na szczeblu Unii Europejskiej znajdują się zarówno w prawie pierwotnym, jak również wtórnym. Prawo pierwotne opiera się w znaczącej mierze na Traktacie ustanawiającym Wspólnotę Europejską, zwłaszcza w omawianym zakresie. Odnośnie prawa wtórnego, uregulowania dotyczące sfery komunikacji elektronicznej oraz jej środków zawarte są w aktach mających charakter wiążący, tj. dyrektywach, rozporządzeniach oraz decyzjach, a nadto w niewiążących zaleceniach, opiniach czy komunikatach. Analiza porządku prawnego Unii Europejskiej w zasadzie jednoznacznie wskazuje, iż zdecydowana większość uregulowań dotyczących telekomunikacji znajduje się w dyrektywach Komisji Europejskiej lub ewentualnie Rady działającej wspólnie z Parlamentem[82]. Niejednokrotnie akty te formułują nowe definicje uprzednio przyjętych pojęć. W kwestii zagadnień teoretycznych w przeszłości, z uwagi na utratę mocy obowiązującej tego aktu, istotne znaczenie przypisywano tzw. dyrektywie ramowej, tj. dyrektywa 2002/21/WE z dnia 7 marca 2002 r. o wspólnych ramach regulacyjnych dla sieci usług komunikacji elektronicznej. Szczególnie istotne znaczenie ma również dyrektywa podjęta na szczeblu Unii Europejskiej, która w sposób bezpośredni wymusiła pewne regulacje na arenie krajowych porządków prawnych. Dyrektywa Komisji 2002/77/WE z dnia 16 września 2002 r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej zobowiązała państwa członkowskie do zniesienia wyłącznych i specjalnych praw do tworzenia oraz dostarczania sieci komunikacji elektronicznej[83].

W zakresie uregulowań podejmowanych na szczeblu unijnym, konieczne jest zasygnalizowanie przełomowego momentu z punktu widzenia społeczeństwa informacyjnego, czyli inicjatywy „eEurope – Społeczeństwo informacyjne dla wszystkich" ogłoszonej w dniu 8 grudnia 1999 r. Program ten jest jednym z najważniejszych elementów polityki Unii Europejskiej w zakresie komunikacji elektronicznej[84]. Komisja Europejska wytyczyła sfery, w których nastąpić powinny przeobrażenia dla zapewnienia rozwoju społeczeństwa

[82] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Business, 2008, s. 71
[83] Ibidem., s. 74
[84] M. Kuliński, *Regulacje Komunikacji Elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej*, CH Beck, Warszawa 2010, s. 23-25

informacyjnego. W przywołanej inicjatywie nacisk położono przede wszystkim na powszechny, szybki i tani dostęp do Internetu, rozwój e-gospodarki, wprowadzenie środków komunikacji elektronicznych do szkół dla zapewnienia rozwoju młodzieży i inne. Następnie sukcesywnie podejmowane były kolejne dokumenty wyznaczające m.in. ramy czasowe dla konkretnych celów, ale także ich sukcesywnego doprecyzowania. Dokumenty dotyczące przywołanych regulacji wskazują, iż sektor komunikacji elektronicznej pełni kluczową rolę w budowie Europejskiego Społeczeństwa Informacyjnego. Nie sposób przy okazji omawiania kwestii prawa wspólnotowego nie wspomnieć o najistotniejszej obecnie regulacji, mającej współcześnie najdonioślejszy wpływ na omawiane zagadnienia oraz bezpośredni wpływ na porządek krajowy, o czym była mowa wyżej przy okazji Projektu ustawy Prawo komunikacji elektronicznej, tj. o dyrektywie Parlamentu Europejskiego i Rady UE 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej[85].

Wskazać należy, iż Europejski Kodeks Łączności Elektronicznej zastąpił cztery obowiązujące dotąd dyrektywy stanowiące tzw. pakiet dyrektyw łączności elektroniczne, tj. dyrektywę ramową, dyrektywę o dostępie, dyrektywę o zezwoleniach oraz dyrektywę o usłudze powszechnej. Analiza aktów prawnych powszechnie obowiązujących w polskim porządku prawnym jak również przyjętych regulacji na szczeblu europejskim w sposób bezpośredni wskazuje, iż prawodawca europejski wyposażony jest w zdolność większego i przede wszystkim szybszego i sprawniejszego reagowania na zmiany jakie wprost wprowadza i dyktuje postęp technologiczny, albowiem przyjęte przez niego akty prawne są zdecydowanie bardziej aktualne i dostosowane do obecnej sytuacji i warunków w sektorze technologicznym. Wprowadzenie Europejskiego Kodeksu Łączności Elektronicznej jest wynikiem dokonanego przez Unię Europejską całościowego przeglądu obowiązujących w Unii Europejskiej ram regulacyjnych i ma na celu przede wszystkim uproszczenie struktury oraz zwiększenie spójności i przejrzystości regulacji sektora komunikacji elektronicznej, ale równie istotna była konieczność dostosowania nowych przepisów do aktualnych realiów rynkowych. Jak wynika wprost z przyjętej regulacji, akt ten miał zostać implementowany do polskiego porządku prawnego w terminie do dnia 21 grudnia 2020 r. Wdrożenie nastąpić ma poprzez przyjęcie dwóch aktów prawnych, tj. nowej ustawy merytorycznej czyli ustawy Prawo komunikacji

[85] Europejski Kodeks Łączności Elektronicznej, 32018L972-EN

elektronicznej[86] (o projekcie której wspominano przy okazji aktów prawnych obowiązujących w krajowym porządku prawnych) oraz odrębnej ustawy zawierającej przepisy wprowadzające.

Europejski Kodeks Łączności Elektronicznej uregulował wiele kluczowych rozwiązań, w tym zwłaszcza w zakresie e-usług, w tym usług świadczonych drogą elektroniczną, wprowadzając szereg definicji legalnych dotychczas problematycznych pojęć, usuwając w ten sposób wątpliwości pojawiające się przy okazji ich interpretacji, a także ujednolicając siatkę pojęciową[87]. Nie sposób omówić i przeanalizować całości regulacji mających istotne znaczenie dla komunikacji elektronicznej i nowych technologii, albowiem jest to temat wymagający odrębnej analizy i badań, niemniej jednak na tle niniejszych rozważań wielokrotnie pojawiać się będą odniesienia do rzeczonego aktu prawnego, zwłaszcza przy okazji potrzeby skonstruowania definicji legalnych pojęć, które wykorzystane zostaną w niniejszej pracy.

2.3. Prawo komunikacji elektronicznej

Prawo komunikacji elektronicznej stanowi jedną z najmłodszych dziedzin prawa[88]. Ocena jego specyfiki prowadzi do jednoznacznego wniosku, iż jest to dziedzina kompleksowa i interdyscyplinarna, łącząca nie tylko elementy prawa prywatnego, ale również prawa publicznego. Filarem jego funkcjonowania, w tym postępu i rozwoju, bez wątpienia jest rozwój technologiczny, w związku z czym prawo komunikacji elektronicznej jest niezwykle dynamicznie rozwijającą się dziedziną prawa. O ile w przypadku innych dziedzin prawa co do zasady wykorzystywane są podobne aparaty pojęciowe, odnoszące się do przynajmniej zbliżonych instytucji, o tyle w przypadku omawianej dziedziny nieco inaczej kształtuje się sytuacja w tym zakresie. Wielokrotnie w aktach prawnych regulujących sferę prawa komunikacji elektronicznej wykorzystywane są terminy, które na potrzeby niniejszej pracy określić można mianem specjalistycznych. Przy omawianiu i regulowaniu instytucji dotyczących tej sfery wykorzystywane są terminy dotyczące informatyzacji, komputerów, technologii oraz urządzeń jej dotyczących. Warto zaznaczyć nadto, iż ciężko jest stworzyć jednolitą siatką pojęciową, pozwalającą na precyzyjne ustalenie znaczenia każdego z pojęć.

---

[86] https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?id=66C7F7C637867159C12589170035C136 (dostęp: 14.02.2023 r.)

[87] D. Adamski, E. Galewska, *Prawo komunikacji elektronicznej* w prawie Unii Europejskiej [w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003, s. 184 i nast.

[88] Szerzej: A. Monarcha-Matlak, *Komunikacja elektroniczna, prawo komunikacji elektronicznej, Europejski kodeks łączności elektronicznej i ich wpływ na rozwój jurysdykcji administracyjnej* [w:] M. Kruś (red.), L. Staniszewska (red.), M. Szewczyk (red.) *Kierunki rozwoju jurysdykcji administracyjnej,* Wolters Kluwer, Warszawa 2022, s. 267 i nast.

Jedynie zaznaczyć należy, iż z uwagi na obecnie kształtującą się sytuację nie tylko w kraju, ale również na świecie, komunikowanie się za pomocą nowych technologii rozwinęło się na potężną skalę. Wspomnieć tutaj należy chociażby o doręczeniach elektronicznych, występujących zarówno w procedurze cywilnej jak i administracyjnej[89], o przełomowym znaczeniu podpisu elektronicznego, umożliwiającego w zakresie administracji państwowej załatwienie niemalże wszystkich spraw i zobowiązań. Nadto zupełna nowość, wzbudzająca niestety wiele kontrowersji, tj. wykorzystywanie telekonferencji, również na rozprawach sądowych[90]. Takich przykładów można byłoby przywoływać zdecydowanie więcej, natomiast w dalszej części pracy zostaną omówione z praktycznego punktu widzenia, ze wskazaniem dokładnych badań obrazujących rzeczywiste ich wykorzystanie, zarówno przez obywateli jak również przez szeroko rozumiane zawody prawnicze.

3. Społeczeństwo informacyjne

Z uwagi na specyficzny charakter dziedziny objętej przedmiotem niniejszej pracy, niejednokrotnie mamy do czynienia z trudnościami w zakresie precyzyjnego i jednoznacznego sformułowania definicji podstawowych pojęć. W przypadku terminu społeczeństwo informacyjne nie sposób znaleźć uniwersalnej jego definicji.

3.1. Pojęcie społeczeństwa informacyjnego

Potrzeba możliwie najpełniejszego ujednolicenia siatki pojęciowej, stwarza konieczność przywołania definicji społeczeństwa informacyjnego na gruncie aktów prawnych regulujących komunikację elektroniczną w najszerszym z możliwych znaczeń. Akty wykonawcze Unii Europejskiej w swoich regulacjach nie odnoszą się bezpośrednio do tego pojęcia. Nie sposób również znaleźć go w przepisach prawa krajowego. Niemniej jednak, pośrednio odnosi się do niego dyrektywa 98/40/WE, która przywołuję definicję usług społeczeństwa informacyjnego, wobec czego z niego można wytypować pewne cechy poszukiwanego znaczenia. Nadto punkt 18 Wstępu dyrektywy 2000/31 Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku

[89] M. Kotulska, *Zakres stosowania środków komunikacji elektronicznej w postępowaniu administracyjnym*, Samorząd Terytorialny 2015/7-8/74-86

[90] Szerzej: M. Żuchowska-Grzywacz, *Mediacja w postępowaniu administracyjnym przy użyciu środków elektronicznych* [w:] M. Kruś (red.), L. Staniszewska (red.), M. Szewczyk (red.) *Kierunki rozwoju jurysdykcji administracyjnej*, Wolters Kluwer, Warszawa 2022, s. 187 i nast.

wewnętrznego[91] opisowo odnosi się do definicji usług społeczeństwa informacyjnego, wskazując, iż obejmują one szeroki zakres rodzajów działalności gospodarczej prowadzonej w trybie online. W tym miejscu prawodawca europejski wyczerpująco wskazuje, co mieści się, a co zostało wykluczone z tego katalogu.

Reasumując powyżej poczynione ustalenia, wskazać należy, iż społeczeństwo informacyjne to takie, w którym większość aktywnych zawodowo osób zajmuje się przetwarzaniem informacji, a narzędzia informatyczne wykorzystywane są szeroko także w związku z innymi formami aktywności obywateli (komunikacją, konsumpcją, edukacją)[92]. Z uwagi na nieustannie rosnące znaczenie sieci teleinformatycznej jako nośnika danych w doktrynie odnajduje się wiele rożnych definicji społeczeństwa informacyjnego, z których każda przykłada największą uwagę do innych – równie ważnych aspektów[93]. W większości definicji jako jedne z najważniejszych determinant tego procesu wymienia się oczywiście informację i dynamiczny rozwój technologii informacyjno-komunikacyjnych[94]. Społeczeństwo informacyjne jest też coraz częściej postrzegane jeszcze szerzej – z punktu widzenia przemian zachodzących w różnych sferach życia[95]. Jako przykład takiej definicji można wskazać tę, zawartą w Strategii rozwoju społeczeństwa informacyjnego w Polsce do roku 2013[96], zgodnie z którą jest to „(…) społeczeństwo, w którym przetwarzanie informacji z wykorzystaniem technologii informacyjnych i komunikacyjnych stanowi znaczącą wartość ekonomiczną, społeczną i kulturową".

Kwestia ta wyczerpująco została poddana analizie przez P. Polańskiego w pracy pt. „Usługi społeczeństwa informacyjnego na tle reformy usług Unii Europejskiej", gdzie autor przywołuje konkretne cechy. Wskazuje m.in. iż charakteryzują się one brakiem równoczesnej obecności stron, elektronicznym charakterem usług, świadczeniem na indywidualne żądanie

[91] Dyrektywa 000/31 Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz. U. UE L 2000.178.1)
[92] G. Szpor, *Urzędnicy w społeczeństwie informacyjnym*, [w:] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2007, s. 288
[93] Szerzej: M. Sokołowski , *Pojęcie usługi społeczeństwa informacyjnego* [w:] M. Dumkiewicz (red.), K. Kopaczyńska-Pieczniak (red.), J. Szczotka (red.), *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie*. Tom I, 2020
[94] R. Seweryn, *Technologie informacyjne i komunikacyjne*, C.H. Beck, Warszawa 2017, s. 14 i nast.
[95] D. Skoczylas, *Aksjologiczny wymiar e-administracji i cyberbezpieczeństwa w kontekście potrzeb jednostki i wspólnoty* [w:] Z. Duniewska (red.), M. Karcz-Kaczmarek (red.), Wilczyński P. (red.), *Prawo administracyjne w służbie jednostki i wspólnoty,* Wolters Kluwer, Warszawa, 2022, s. 207 i nast.
[96] Społeczeństwo informacyjne w Polsce w 2019 roku, 21.10.2019 r., dostępny w internecie: stat.gov.pl dostęp 28.02.2020 r.

strony[97]. Przywołane cechy zdecydowanie pokazują, iż usługi społeczeństwa informacyjnego są niezwykle ściśle związane właśnie z komunikacją elektroniczną i identyfikującymi ją środkami, o czym świadczą analogiczne cechy tych definicji.

Reasumując, potrzeba dostępu do informacji, która silnie pojawiła się w XX wieku, zainicjowała również konieczność nowego charakteryzowania społeczeństwa, które sukcesywnie zaczęło przejawiać ogromne różnice w stosunku do tego, które przyjęto przed XX końcem XX wieku. Informacja jako decydujący czynnik produkcyjny z pewnością definiuje społeczeństwo informacyjne. Pierwotnie idea społeczeństwa informacyjnego była ideałem, który zmierza do przełomowej zmiany cywilizacji, sukcesywnie jednak zmieniając wymiar reform. Społeczeństwo informacyjne bez najmniejszych wątpliwości ma służyć samemu społeczeństwu, polepszając jego byt, mocno ułatwiając funkcjonowanie w nim. W zakresie regulacji prawa krajowego odnoszącego się do społeczeństwa informacyjnego nie sposób się nie odnieść do uchwały Sejmu Rzeczpospolitej Polskiej z dnia 14 stycznia 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce[98]. Przywołany akt prawny dotyczył powszechnego dostępu do Internetu, jego wykorzystania, planów i priorytetów w zakresie rozwoju społeczeństwa informacyjnego, ale również systemów teleinformatycznych w administracji, przy poszanowaniu systemów dotyczących bezpieczeństwa w sieci oraz bezpieczeństwa i obronności państwa.

Społeczeństwo informacyjne opiera się na komunikacji elektronicznej[99]. Nie ma w zasadzie wątpliwości co do tego, iż rozwój społeczeństwa komunikacyjnego pociąga za sobą konieczność pewnych zmian technologicznych. Respektowanie zasad bezpieczeństwa, które mają zapobiegać popełnianiu przestępstw w sieci wymaga odpowiedniej korelacji pomiędzy urządzeniami służącymi do komunikacji i oprogramowania. Oczywiście nie bez znaczenia pozostają w tej kwestii regulacje prawne, które zapewniają pewność i bezpieczeństwo obrotu, ale również dostępu do informacji i korzystania z nich, a nadto dbają o ochronę danych osobowych.

W wyniku licznych przeobrażeń w sferze społeczeństwa informacyjnego, w doktrynie pojawiły się nowe rodzaje szeroko rozumianej demokracji. W związku z niepodważalnym

[97] P. Polański, *Usługi społeczeństwa informacyjnego na tle reformy usług Unii Europejskiej*, Quo Vafis Europo, Warszawa 2014, s. 241-260
[98] Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce (M.P. 2000 nr 22 poz. 448)
[99] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer business, 2008, s. 48

faktem, iż rozwój technologiczny oraz pojawienie się komunikacji elektronicznej wywiera ogromny wpływ na funkcjonowanie społeczeństwa, nie ma wątpliwości co do tego, iż zarówno życie społeczne jak i sfera relacji obywatel-państwo zaczyna przybierać nieco odmienny (niż np. XX-wieczny) model. W literaturze zgodnie przyjmuje się, iż na kanwie wyżej poczynionych ustaleń pojawił się model demokracji elektronicznej[100]. W podstawowym znaczeniu uznać można, iż jest to nic innego, jak demokracja wykorzystująca w relacji z obywatelami środki komunikacji elektronicznej, zwłaszcza Internet.

W doktrynie w ramach elektronicznej demokracji wyróżnia się trzy jej kategorie. Pierwsza z nich to teledemokracja[101], w przypadku której decydujące wykorzystywanie w procesie komunikacji elektronicznej telewizję. Kategoria ta miała duże zastosowanie w drugiej połowie XX wieku, kiedy telewizja była łącznikiem i przekaźnikiem informacji pomiędzy władzą a obywatelem. Druga kategoria to cyberdemokracja[102] wykorzystująca zwłaszcza komputery oraz ostatnia kategoria, czyli elektroniczna demokratyzacja[103], której podstawowym założeniem jest bezpośredni dostęp do każdej możliwej informacji. Nie ma wątpliwości co do tego, iż postęp technologiczny wymusza niejako rozwój społeczeństwa informacyjnego. Dzięki dostępowi do sieci, współcześnie, za pomocą odpowiednich systemów teleinformatycznych oraz przy wykorzystaniu urządzeń elektronicznych, mamy natychmiastowy dostęp do danych sądowych, w postaci orzeczeń, ogłoszeń itp. Za pomocą sieci Internetowej udostępniane są również wzory dokumentów, formularze. Współcześnie telekomunikacja jest podstawową infrastrukturą gospodarki. Rozwój w tym sektorze powoduje bezpośrednio postęp w innych sferach gospodarczych. Informatyzacja wielu aspektów we współczesnym świecie implikuje konieczność stwierdzenia, iż żadna dziedzina życia społecznego, ale nie tyko społecznego, nie może prawidłowo funkcjonować bez odpowiednio przystosowanej i rozwiniętej infrastruktury telekomunikacyjnej[104]. Demokracja elektroniczna najsilniej widoczna jest w społeczeństwie amerykańskim, co w zasadzie nie budzi większego zdziwienia, jako że przyjąć można, iż właśnie tam miała swoje korzenie. Wykorzystywanie Internetu, zwłaszcza w procesach wyborczych, przyniosło satysfakcjonujące rezultaty, mając zwłaszcza na uwadze, iż badania

[100] A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer business, 2008, s. 48

[101] M. Kuliński, *Regulacje Komunikacji Elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej*, CH Beck, Warszawa 2010, s. 48-49

[102] Szerzej: J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Wolters Kluwer, 2020

[103] M. Kuliński, *Regulacje Komunikacji Elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej*, CH Beck, Warszawa 2010, s. 48-49

[104] M. Kuliński, *Regulacje Komunikacji Elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej*, CH Beck, Warszawa 2010, s. 18

wykazały, że wówczas więcej wyborców wzięło czynny udział w wyborach demokratycznych. Uzasadnione jest to przede wszystkim łatwiejszym i bezpośrednim, natychmiastowym dostępem do informacji o kandydatach, ale także możliwość dalszego wyszukiwania informacji w Internecie, będące niejako konsekwencją uzyskanej wiedzy o kandydatach.

3.2. Środki komunikacji elektronicznej

Pojęcie środek komunikacji elektronicznej, w odniesieniu do części z wyżej przytoczonych pojęć, jest definicją legalną. Art. 3 pkt 4 ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne odsyła do art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[105]. Wskazana ustawa wprowadziła do porządku prawnego wiele istotnych z punktu widzenia omawianych materii pojęć, w tym bardzo istotne pojęcie „środka komunikacji elektronicznej". Interpretacja przywołanych regulacji pozwala na przyjęcie, iż środki komunikacji elektronicznej to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumienia się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi[106]. Na istotny charakter tego pojęcia wskazuje fakt, iż ustawodawca przywiązał dużą wagę do jednolitego rozumienia tego pojęcia w aktach normatywnych. Ustawą z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej zrealizowano nałożony na Radę Ministrów w art. 62 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne obowiązek dostosowania terminologii w przepisach odrębnych ustaw dotyczących informatyzacji do określeń „informatyczny nośnik danych" oraz „dokument elektroniczny"[107]. Postanowienia rzeczonej ustawy wprowadziły do Kodeksu postępowania administracyjnego wiele uregulowań umożliwiających elektroniczną komunikację z organami administracji publicznej, w tym jest z aktualnie najbardziej popularnych sposobów doręczeń, to jest doręczenia za pomocą środków komunikacji elektronicznej.

Powyższe rozważania wskazują, iż środki komunikacji elektronicznej są to metody, narzędzia umożliwiające komunikowanie się na odległość, za pomocą szeroko rozumianych urządzeń elektronicznych. Cechę konstytutywną środków komunikacji elektronicznej stanowi

[105] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
[106] G. Szpor [w:] *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz,* Wolters Kluwer Business, 2015, s. 58
[107] P. Chmieliński, *Środki komunikacji elektronicznej wykorzystywane w postępowaniu administracyjnych,* Przegląd Prawa Publicznego 2015//11/38-48

realizacja procesu komunikowania się przy wykorzystaniu transmisji danych między systemami teleinformatycznymi[108]. Analiza wyżej przytoczonej definicji legalnej bezpośrednio wskazuje na fakt, iż komunikacja taka musi dotyczyć konkretnie oznaczonych podmiotów, a porozumiewanie się powinno dotyczyć co najmniej dwóch[109]. Generalnie rzecz ujmując w porozumiewaniu się na odległość chodzi o potencjalną możliwość przekazania informacji bez jednoczesnej obecności obu stron[110]. Ustawodawca nie przewiduje przykładów środków komunikacji elektronicznej, z wyjątkiem podstawowego w postaci poczty elektronicznej. Niemniej jednak do katalogu tego zaliczyć można również wiadomości tekstowe SMS i MMS, komunikatory społecznościowe takie jak WhatsApp lub Messenger. Wskazane środki komunikacji elektronicznej oparte są na funkcjonowaniu urządzeń informatycznych oraz właściwego oprogramowania w połączeniu z działaniem sieci telekomunikacyjnej, przy czym dają możliwość przetwarzania, przechowywania, przesyłania i odbierania danych za pomocą telekomunikacyjnego urządzenia końcowego[111]. Niezależnie od powyższego, pomimo bardzo szerokiego katalogu środków komunikacji elektronicznej, możliwości ich wykorzystania w postępowaniu administracyjnym są bardzo ograniczone. Aktualnie najpopularniejszym rozwiązaniem zdaje się być wykorzystanie elektronicznej Platformy Usług Administracji Państwowej (e-PUAP).

Wskazać zatem należy iż środkiem komunikacji elektronicznej realizacji założeń podstawowej w tym zakresie ustawy, tj. ustawy o świadczeniu usług drogą elektroniczną, jest w szczególności poczta elektroniczna oraz zbliżone technologie. W doktrynie wskazuje się na funkcjonalny charakter tego pojęcia, albowiem w kontekście art. 10 rzeczonej ustawy jest identyfikacja technologii, które mogą ingerować w szeroko rozumianą prywatność poprzez niezamówiony przekaz[112]. Reasumując zatem analizę pojęcia środków komunikacji elektronicznej, wskazać należy, iż ustawodawca definiując przywołane pojęcie wprowadził w zasadzie cztery przesłanki, których kumulatywne spełnienie jest wymagane dla przyjęcia danego rozwiązania. Musi być to rozwiązanie techniczne pozwalające na porozumiewanie się na odległość, wykorzystujące transmisję danych między systemami teleinformatycznymi. Co prawda nie ma definicji legalnej pojęcia transmisji danych, niemniej jednak przyjąć należy,

[108] X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004 r., s. 73
[109] D. Lubasz (red.), Namysłowska M. (red.), *Komentarz do ustawy o świadczeniu usług drogą elektroniczną* [w:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw,* Lexis Nexis 2011
[110] D. Szostek, *Czynność prawna a środki komunikacji elektronicznej*, Kraków 2004, s. 35-36
[111] Ibidem.
[112] M. Gomularz, *Świadczenie usług drogą elektroniczną. Komentarz*, Wolters Kluwer, Warszawa 2019, s. 19 i nast.

iż jest to proces przesyłania danych. Aby uznać określone rozwiązanie techniczne za środek komunikacji elektronicznej, konieczne jest, aby umożliwiało przesyłanie danych z jednego systemu teleinformatycznego do innego systemu teleinformatycznego[113]. Ustawodawca zdecydował się na podanie jednego przykładu rzeczonego środka, tj. poczty elektronicznej, rezygnując w ten sposób z kazuistycznego definiowania pojęcia.

Pojęcie systemu teleinformatycznego zostało zdefiniowane w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną jako zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzania i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy Prawo telekomunikacyjne. Definicja tego pojęcia omówiona została również na tle ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, a także w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[114], w której wskazuje się, iż jest to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Mając na względzie wyżej przytoczone definicje, które są jedynie kilkoma z wielu, przyjąć należy z praktycznego punktu widzenia, iż system teleinformatyczny służy do przekazywania danych, ale również ich gromadzenia i przechowywania. Jest to zatem niezbędny element w procesie komunikacji elektronicznej, którego doskonalenia poprawia jakość dostępu do informacji, a w konsekwencji jej jakości.

Przy okazji omawiania specyfikacji środków komunikacji elektronicznej jednoznacznie należy zaznaczyć konieczność odróżnienia tego pojęcia od informatycznego nośnika danych[115]. Zgodnie z definicją legalną przyjętą w art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, informatyczny nośnik danych to materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej. Nośnik danych spełnia zupełnie odmienne funkcje i całkowicie inny jest jego cel. Służy on albowiem do trzech podstawowych czynności, tj. zapisanie,

[113] D. Lubasz, M. Namysłowska, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną w: Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, Wolters Kluwer, Warszawa 2011

[114] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922, z 2018 r. poz. 138, 723)

[115] P. Chmieliński, *Środki komunikacji elektronicznej wykorzystywane w postępowaniu administracyjnych*, Przegląd Prawa Publicznego 2015//11/38-48; Szerzej: G. Szpor, *Lex informatica - problemy słownika* (w:) *Informatyzacja postępowania sądowego i administracji publicznej*, red. J. Gołaczyński, Warszawa 2010

przechowywanie oraz w konsekwencji odczytywanie danych[116]. Natomiast główną funkcją środków komunikacji elektronicznej nie są powyższe operacje, a po prostu przekazywanie informacji na odległość, czyli w dużym uproszczeniu komunikacja elektroniczna, nie wymagająca jednoczesnej obecności adresata i odbiorcy komunikatu[117].

3.3. Technologie mobilne

Nieustannie odnotowywany postęp technologiczny, w tym w zakresie technologii informatycznych zdeterminował możliwość wyodrębnienia nowego jej rodzaju, tj. technologii mobilnych, które obecnie należą do najszybciej rozwijających się[118]. W życiu codziennym współczesnego społeczeństwa, na niemal wszystkich jego płaszczyznach zauważalne jest ich szerokie wykorzystanie. W zasadzie jednogłośnie wskazuje się, iż urządzeniem powodującym maksymalną popularyzację tych technologii jest telefon komórkowy. Za szeroką akceptacją oraz popularyzacją technologii mobilnych przemawia brak ograniczenia w zakresie miejsca korzystania z e-usług, bezpośredniość, natychmiastowość, zdolność do szybkiego podłączenia[119]. Przy okazji tych urządzeń, społeczeństwo informacyjne osiągnęło kolejny, wyższy poziom, zapewniając sobie możliwość bycia online nie tylko zawsze, ale również wszędzie. Wykorzystanie technologii mobilnych, w tym m.in. sieci teleinformatycznej, sieci WiFi, GPS stwarza możliwość pozyskiwania, ale również przesyłania informacji przy wykorzystaniu nowych metod w różnych dziedzinach życia społecznego[120].

Niezwykle ciekawym zagadnieniem i problemem badawczym wartym zasygnalizowania przy okazji omawiania kwestii związanych z rozwojem technologii elektronicznych oraz ich wpływem na zawody prawnicze, jest zasada jawności w postępowaniu sądowym, a wykorzystanie komunikacji elektronicznej[121]. Zasada jawności w procesie sądowym, zwłaszcza karnym pełni szereg ważnych funkcji, w tym funkcję kontrolną

[116] G. Szpor *Art. 3 Objaśnienia określeń użytych w ustawie* [w:] Cz. Martysz (red.), G. Szpor (red.), K. Wojsyk (red.), *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz,* Wolters Kluwer, 2015, s. 49 i nast.
[117] S. Kotecka [w:] *Informatyzacja postępowania sądowego w prawie polskim i wybranych państw*, red. J. Gołaczyński, Biblioteka Sądowa, s. 208
[118] Szerzej: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Wolters Kluwer, Warszawa 2015, s. 38 i nast.
[119] Ł. Łysik, R. Kutera, *Technologie mobilne jako determinanta rozwoju innowacyjnego społeczeństwa informacyjnego,* Ekonomiczne Problemy Usług nr 105, 33-44, 2013 s. 35 i nast.
[120] Szerzej: M. Białecki (red.), S. Kotas-Turoboyska (red.), F. Manikowski (red.), J. Słyk (red.), E. Szczepanowska (red.), *Rozstrzyganie spraw cywilnych. Aktualne wyzwania i perspektywy*, Wolters Kluwer, Warszawa 2022
[121] Por. A. M. Arkuszewska, *Informatyzacja postępowania arbitrażowego,* Wolters Kluwer, 2019, s. 99 i nast., M. Uliasz, *Zasada jawności sądowego postępowania egzekucyjnego w dobie informatyzacji*, Wolters Kluwer, Warszawa, 2019, s. 196 i nast.

zapewniającą transparentność działań organów orzekających oraz ewentualnie innych instytucji zaufania publicznego (w szerokim ujęciu), funkcję wychowawczą w tym również prewencyjną, pozwalającą w ten sposób wpłynąć na społeczeństwo i kształtowanie właściwych postaw i wzorców zachowań, ale również bardzo istotną funkcję gwarancyjną[122]. Nie budzi wątpliwości, iż sposób realizowania zasady jawności zmienia się wraz z rozwojem technologii. Dawniej na salach rozpraw ewidentnie widoczne były tzw. osoby obce, nie będące stronami danego postępowania. Obecnie dostrzegalne są zmiany w tym zakresie, albowiem zdarza się to co raz rzadziej, co oczywiście nie oznacza, iż zmniejszyło się zainteresowanie obywateli postępowaniami, zwłaszcza karnymi. Tymczasem rozwój technologii sprawił, iż zasada jawności realizowana jest w tzw. pośredniej formie, zazwyczaj za pośrednictwem telewizji oraz Internetu[123]. Nieustająca konwergencja mediów sprawia, iż za ich pomocą obywatele niejako sprawują kontrole nad prowadzonymi postępowaniami. Problematyka ta jednoznacznie pozwala stwierdzić, iż rozwój technologii elektronicznych wpływa bezpośrednio na wiele aspektów życia codziennego, ale również na niemalże każdą sferę prawniczą, w tym wymiaru sprawiedliwości. Budzącym wiele kontrowersji jest zagadnienie dotyczące przekazywania informacji za pomocą technologii elektronicznych, zwłaszcza mediów oraz zaburzania w ten sposób zasady jawności. Nie ulega w zasadzie wątpliwości, iż sposób przekazania informacji, ich ilość oraz jakość w zdecydowanej większości zależy od punktu widzenia, w tym prezentowanych poglądów politycznych oraz kulturowych. Teoretycznie media cechować się winny neutralnością, niezależnością oraz bezstronnością, natomiast wszelkie niesnaski w tym zakresie nie będą objęte przedmiotem niniejszej pracy. Warto jednakże zauważyć, że każdorazowe zniekształcenie informacji dotyczących szeroko rozumianych procesów, może mieć poważne i ujemne konsekwencje, chociażby z punktu widzenia kontroli społeczeństwa nad organami orzekającymi, jak również ich działaniami.

3.4. E-usługi, usługa świadczona drogą elektroniczną, usługa społeczeństwa informacyjnego

W ramach komunikacji elektronicznej pojawia się szereg pojęć specjalistycznych, które wymagają krótkiego omówienia. Częścią procesu komunikacji w formie elektronicznej są sieci i usługi informacyjne. W ramach sieci teleinformatycznej wyróżnia się również sieć komputerową, składającą się z stacji sieciowych oraz kabla sieciowego, umożliwiającego

[122] M. Zimna, *Wyłączenie jawności rozprawy jako gwarancja ochrony interesów uczestników postępowania karnego*, Prokuratura i Prawo 2016/9/87-108
[123] Szerzej: A. Machnikowska, *Zasada jawności w postępowaniu procesowym – modernizacja czy marginalizacja? Wybrane zagadnienia*, Polski Proces Cywilny 2022/1/80-124

dostęp do zasobów informacji. Uznać bez wątpienia należy, iż Internet to globalna sieć komputerowa. Realizacja systemów występujących w ramach e-usług wymaga uprzedniego odpowiedniego przygotowania, w tym m.in. poprzez zaprojektowanie i oprogramowanie odpowiednich systemów informatycznych. W dobie szczególnego nacisku na ochronę danych osobowych oprogramowania te podlegają szczególnemu doprecyzowaniu w tym zakresie, aby możliwie najpełniej chronić korzystające z nich podmioty. W doktrynie przyjmuje się, iż e-usługi mogą być realizowane co najmniej na dwa sposoby, tj. poprzez produkt cyfrowy lub poprzez usługę cyfrową[124]. Wskazać nadto należy, iż e-usługi rozumieć należy jako usługi świadczone w sposób całkowicie automatyczny, bez najmniejszego udziału siły człowieka[125]. Oczywiście owa automatyczność realizowana jest właśnie za pomocą wspomnianych na wstępie odpowiednio przygotowanych oprogramowani i systemów. Z przyjętym w przywołanej definicji elementem wskazującym na zupełny brak udziału człowieka w procesie e-usługi nie w pełni należy się zgodzić, albowiem czynnik ludzki jest niezbędny chociażby przy inicjacji tego procesu. Niejednokrotnie systemy zawodzą, generując usterki, wówczas również niezbędna jest pomoc człowieka, podobnie w zakresie np. wprowadzenia pewnych danych.

Na tle niniejszych rozważań jedną z najistotniejszych definicji wprowadzonych na mocy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[126] jest pojęcie świadczenia usługi drogą elektroniczną, które zestawić należy z pojęciem usługi społeczeństwa informacyjnego. Kwalifikacja prawna usług z pogranicza łączności elektronicznej i społeczeństwa informacyjnego w zasadzie od lat determinuje wiele problemów. Nieustannie prosperujący rozwój technologiczny doprowadził do wzrostu efektu konwergencji mediów, co z kolei doprowadziło do zatarcia granic ustalonych przez prawodawcę unijnego, w szczególności między usługą przesyłu sygnału a usługą społeczeństwa informacyjnego świadczą w oparciu o ten przesył[127]. Dyrektywa UE 2015/1535[128] w art. 1 ust. 1 lit. b definiuje usługę społeczeństwa informacyjnego jako usługę normalnie świadczoną za wynagrodzeniem na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Reasumując

[124] A. Bytniewski, *Wpływ systemów informatycznych na rozwój społeczeństwa informacyjnego*, Ekonomiczne Problemy Usług nr 105, 13-21, 2013, s. 16 i nast.
[125] E. Nowińska, *Komentarz do art. 10 ustawy o świadczeniu usług drogą elektroniczną* [w:] E. Nowińska (red.) K. Szczepanowska-Kozłowska (red.) *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, wyd. II, Wolters Kluwer, 2022
[126] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
[127] M. Ciechomska, *E-usługi a RODO*, Wolters Kluwer, 2021, s. 113-118
[128] Dyrektywa UE 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. U. UE L 2015.241.1)

przytoczoną definicję wskazać należy, iż usługi społeczeństwa informacyjnego, aby mogły zostać zakwalifikowane do takich usług muszą spełniać kumulatywnie trzy kryteria:

1. świadczenie na odległość, tj. usługa świadczona bez równoczesnej obecności stron, czyli brak fizycznej obecności stron zapewniającej bezpośredni kontakt w danej chwili i w konkretnym miejscu;
2. świadczenie usługi drogą elektroniczną, tj. usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych[129];
3. świadczenie usługi na indywidualne żądanie odbiorcy usług; załącznik I do dyrektywy 2015/1535 wskazuje na usługi, które nie są świadczone w ten sposób, określając, iż są to usługi świadczone w formie przesyłania danych bez indywidualnego zamówienia i przeznaczone do równoczesnego odbioru przez nieograniczoną liczbę odbiorców (m.in. usługi rozpowszechniania telewizyjnego, usługi przesłania sygnału radiowego, teletekst telewizyjny).

Warte uwagi jest również wspomnienie o kazuistycznym opracowaniu pojęcia na kanwie załącznika V do dyrektywy 98/34/WE[130] w brzmieniu nadanym dyrektywą 98/48/WE, który przytacza przykładowy katalog usług, które zdaniem prawodawcy nie mogą być klasyfikowane jako usługi społeczeństwa informacyjnego, albowiem pomimo korzystania z urządzeń elektronicznych nie spełniają one jednego z obligatoryjnych wyżej opisanych wymogów, tj. warunku usługi świadczonej na odległość bez fizycznej obecności dostawcy i odbiorcy badanie lekarskie lub wykonywanie zabiegów lekarskich w gabinecie lekarskim z zastosowaniem urządzeń elektronicznych przy fizycznej obecności pacjenta; wgląd do elektronicznego katalogu w sklepie przy fizycznej obecności klienta; rezerwacja biletu lotniczego w biurze podróży przy fizycznej obecności klienta za pomocą sieci internetowej; udostępnienie gier elektronicznych w salonie przy fizycznej obecności użytkownika.

Proces analizy oraz badanie kwestii zależności pojęć usługi społeczeństwa informacyjnego oraz usługi świadczonej drogą elektroniczną determinuje konieczność przyjęcia, iż oba pojęcia

[129] Por. wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 24 czerwca 2020 roku sygn. III SA/GI 138/20, LEX nr 3040660

[130] Dyrektywa 98/48/WE Parlamentu Europejskiego i Rady z dnia 20 lipca 1998 r. zmieniająca dyrektywę 98/34/WE ustanawiającą procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz. U. UE.L.1998.217.18)

mają wspólny zakres definicyjny. Istotna i w zasadzie jedyna różnica sprowadza się do elementu odpłatności usługi, którego nie umieszczono w przypadku definiowania pojęcia usługi świadczonej drogą elektroniczną. Niemniej jednak w doktrynie wskazuje się, iż pomimo niewprowadzenia wprost tego elementu w ustawie o świadczeniu usług drogą elektroniczną, jest on również istotny w przypadku tej usługi[131]. Kwestia odpłatności usługi nie powinna być spłycana wyłącznie do kwestii wynagrodzenia pieniężnego, albowiem może dotyczyć również innej kategorii profitów chociażby w postaci możliwości przetwarzania danych osobowych, co potwierdza orzecznictwo Trybunału Sprawiedliwości[132].

4. Sztuczna inteligencja

Z uwagi na widocznie zauważalny nieustanny rozwój środków komunikacji elektronicznej oraz jego wpływ na pozyskiwanie i przekazywanie informacji, co w połączeniu z zarządzaniem wiedzy jest fundamentem społeczeństwa informacyjnego, poruszyć należy kwestię sztucznej inteligencji. Problematyka *Artificial Intelligence*, zwłaszcza w aspekcie uregulowań prawnych oraz sfery etycznej, budzi wiele zastrzeżeń i wątpliwości. Dyskusja ta po opublikowaniu w lutym 2017 r. rezolucji Parlamentu Europejskiego zawierającej zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki[133] stała się jeszcze bardziej aktywna. Głównym zastrzeżeniem była kwestia ewentualnej odpowiedzialności z punktu widzenia prawa oraz etyki[134]. Na arenie Unii Europejskiej przyjęto dotychczas szereg rozwiązań prawnych bezpośrednio odnoszących się do kwestii sztucznej inteligencji, w tym m.in. Rezolucję Parlamentu Europejskiego z dnia 3 maja 2022 r. w sprawie sztucznej inteligencji w epoce cyfrowej[135]. Nie ma w zasadzie wątpliwości co do stwierdzenia, iż każde przeobrażenia w sferach życia codziennego wymagają odpowiedniego dostosowania do nich przepisów prawnych, aby zapobiec ewentualnym wątpliwościom przy okazji chociażby powstałych szkód, czy właśnie kwestii odpowiedzialności etycznej. Unia Europejska za cel ustanowiła przyjęcie do końca 2023 r. kompleksowego aktu dotyczącego sztucznej inteligencji. W tym zakresie ma powstać pierwszy pakiet przepisów odnoszących się do szans i zagrożeń

[131] M. Gomularz, *Świadczenie usług drogą elektroniczną. Komentarz. Wolters Kluwer*, Warszawa 2019, s. 19 i nast.
[132] Por. wyrok Trybunału Sprawiedliwości z dnia 11 września 2014 r. sygn. C-291/13, EU:C:2014:2209, pkt 28, 29.
[133] Rezolucja Parlamentu Europejskiego zawierającej zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL))
[134] https://www-arch.polsl.pl/wydzialy/ROZ/ZN/Documents/zeszyt%20123/Stylec-Szromek.pdf (dostęp: 10.03.2023 r.)
[135] Rezolucja Parlamentu Europejskiego z dnia 3 maja 2022 r. w sprawie sztucznej inteligencji w epoce cyfrowej (Dz. U. UE. C.2022.465.65)

jakie niesie za sobą sztuczna inteligencja, przy zapewnieniu możliwie najbardziej przyjaznego środowiska dla rozwoju firm, naukowców i przedsiębiorstw w tym zakresie. Parlament powołał specjalną Komisję ds. Sztucznej inteligencji w erze cyfrowej (AIDA). Składa się ona z 33 członków i jest powołana celem analizowania przyszłego wpływu sztucznej inteligencji w erze cyfrowej na gospodarkę UE, w szczególności na umiejętności, zatrudnienie, technologie finansowe, edukację, zdrowie, transport, turystykę, rolnictwo, środowisko, obronę, przemysł, energię i rząd. Jak wynika z danych przedstawionych przez Unię Europejską, rozwój sztucznej inteligencji może dostarczyć nawet 60 mln nowych miejsc pracy na całym świecie do 2025 r. W odniesieniu do omawianych zagadnień istotny jest również nowy akt prawny podjęty na arenie Unii Europejskiej, to jest akt o sztucznej inteligencji (AI Act) Parlamentu Europejskiego, ostatecznie przyjęty w dniu 14 czerwca 2023 roku, znaczną większością głosów. Co istotne, w akcie tym dodano nowe przepisy, aby uwzględnić sytuacje, w których systemy sztucznej inteligencji mogą być wykorzystywane do wielu różnych celów (sztuczna inteligencja ogólnego przeznaczenia) i w których technologia sztucznej inteligencji ogólnego przeznaczenia jest następnie włączana do innego systemu wysokiego ryzyka. Nadto wprowadzono szereg zmian do przepisów dotyczących wykorzystywania systemów sztucznej inteligencji do celów egzekwowania prawa, aby uwzględnić szczególne cechy organów ścigania. Celem ich wprowadzenia jest zapewnienie potrzeby poszanowania poufności szczególnie chronionych danych operacyjnych w związku z działalnością tych organów[136].

Z pełną odpowiedzialnością stwierdzić należy, iż sfera sztucznej inteligencji jest najszybciej rozwijającą się technologią. Przyjmuje się, iż w związku z tym o 400% w ostatniej dekadzie wzrosła liczba opublikowanych zgłoszeń patentowych w omawianej dziedzinie. Chęć przyspieszenia, ulepszenia oraz przede wszystkim zminimalizowania kosztów powoduje ogromne inwestycje lokowane właśnie w rozwój tej sfery. Z danych przedstawionych przez Komisję Europejską[137] wynika, iż w Ameryce Północnej inwestycje w prospekt sztucznej inteligencji w 2016 r. wyniosły 12,1-18,6 mld euro, w Azji 6,5-9,7 mld euro, zaś w Europie 2,4-3,2 mld euro. Dane szacunkowe wskazują natomiast, iż do 2025 r. 6500-12 000 mld euro rocznie będzie inwestowane w gospodarkę automatyzacji opartą o działanie maszyn, w tym sztucznej inteligencji. Gwałtowny i dynamiczny rozwój omawianej sfery, w przyszłości bezpośrednio wpłynąć może na byt i funkcjonowanie różnych zawodów, w tym również zawodów prawniczych. W zależności od tego z jaką sferą i gałęzią aktualnie będziemy mieli

[136] R. Bujalski, *Akt o sztucznej inteligencji [Projekt UE] Komentarz praktyczny*, LEX, 2022
[137] Źródło: Komisja Europejska (2019), IPOL (2020)

do czynienia, inaczej przedstawiała będzie się definicja sztucznej inteligencji, bowiem wówczas jej zastosowanie będzie zupełnie inne. Przyjąć należy dwa poglądy w zakresie funkcjonowania sztucznej inteligencji. Pierwszy wskazuje, iż jest to byt stworzony z myślą o rozwiązywaniu określonych zadań, zaś drugi określa sztuczną inteligencję jako podmiot obdarzony samoświadomością[138]. Drugie podejście na tle niniejszej pracy i rozważań poruszanych na jej gruncie jest zbyt daleko idące. Pozytywne i pełne nadziei spojrzenie na tą problematykę pozwala uznać, iż inteligencja i siła człowieka nie jest możliwa do pełnego zastąpienia przez sztuczną inteligencję. Konieczność dynamicznego przystosowania się do danej, niespodziewanej sytuacji, niejednokrotnie wymuszającej nagłej zmiany myślenia oraz decyzji wzmacnia przyjęte stanowisko. Potencjał sztucznej inteligencji wykorzystywany jest co do zasady w odniesieniu do maszyn, które bez wątpienia funkcjonują według narzuconego im schematu, są odpowiednio zaprogramowane i o ile niejednokrotnie wyposażone są w możliwości adaptacyjne czy zdolności uczenia się, o tyle może doprowadzić do rezultatów odmiennych od zamierzonych, albowiem nie jest to urządzenie zdolne do myślenia. Idealistyczne spojrzenie na tę kwestię powoduje bezpośrednio wyobrażenie o sztucznej inteligencji stworzonej na wzór ludzkiego mózgu, natomiast realnie rzecz biorąc mocno zderzy się to z rzeczywistością, albowiem okoliczność ta jest niemalże niemożliwa do przyjęcia.

Widocznie dostrzegalny postęp technologiczny we wszystkich sferach życia społecznego prowadzi do uznania, iż robotyzacja w wielu dziedzinach jest wręcz nieunikniona. Analiza ,i obserwacja otoczenia jednoznacznie wskazuje, iż praca i wysiłek człowieka zostaje zastąpiona rozmaitymi maszynami. Każde zawody, w mniejszym lub większym stopniu, zagrożone są robotyzacją. W literaturze wskazuje się, iż na podstawie badań ryzyko to w przypadku zawodu sędziego wynosi 3%[139]. Analiza potencjalnego zagrożenia zastąpieniem sztucznej inteligencji zawodów prawniczych zostanie poczyniona w odrębnym rozdziale, z dwóch punktów widzenia: idealistycznego oraz realnego.

5. Administracja elektroniczna jako część administracji publicznej

Pomimo wyżej przedstawionej „ogólnej" definicji pojęcia informacja, na kanwie sfery administracji publicznej[140], wykorzystującej w swojej procedurze informacje w każdym

[138] S. Tkacz, Z. Tobor, *Prawo a nowe technologie, Wydawnictwo Uniwersytetu Śląskiego*, Katowice 2019, s. 52
[139] S. Tkacz, Z. Tobor, *Prawo a nowe technologie, Wydawnictwo Uniwersytetu Śląskiego*, Katowice 2019, s. 52
[140] Szerzej: J. Blicharz (red.), L. Zacharko (red.) *Administracja. Prawo administracyjne. Część ogólna*, Katowice 2018; J. Blicharz J. (red.), L. Zacharko (red.), *Administracja. Prawo administracyjne. Część ogólna*, Katowice 2018

aspekcie, przyjmuje się nowe znaczenie informacji[141]. W literaturze[142] wskazuje się, iż informacja w administracji publicznej to „wiedza odnosząca się do podmiotów, przedmiotów, działań, faktów czy stanów, która stanowi istotny czynnik umożliwiający działania organów administracji publicznej lub efekt tych działań". W tym miejscu zasygnalizować jedynie należy definicję pojęcia administracji publicznej, które to pojęcie będzie wielokrotnie wykorzystywane w dalszej części pracy. Pojęcie to może być rozpatrywane zarówno w aspekcie podmiotowym jak i przedmiotowym, przy czym przyjmując kryterium podmiotowe administracja publiczna jest systemem instytucji działających wedle przyjętych założeń organizacyjnych. Z kolei kryterium przedmiotowe pozwala na przyjęcie, iż w zakres administracji publicznej wchodzi zarówno organizowanie usług publicznych, jak i tworzenie bazy materialnej i świadczenie tych usług[143].

Zgodnie z podstawowymi zasadami zawartymi w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne podmioty publiczne, używając środków komunikacji elektronicznej do przekazywania informacji podmiotom z kręgu poza administracji rządowej, obowiązane są do zapewnienia, aby wykorzystywane do tego systemy teleinformatyczne spełniły wymóg równego traktowania rozwiązań informatycznych. Zasada neutralności znajduje swoje odzwierciedlenie w przepisach konstytucyjnych, zgodnie z którymi wszyscy są równi wobec prawa i mają prawo do równego traktowania przez organy władzy publicznej. Zgodnie z brzmieniem art. 13 ust. 2 pkt 2 ww. ustawy sposobem udostępniania przez podmioty publiczne m.in. dokumentów elektronicznych, danych, protokołów komunikacyjnych szyfrujących oraz testów akceptacyjnych jest m.in. ich publikowanie w Biuletynie Informacji Publicznej, czyli urzędowym publikatorze teleinformatycznym. Szczegółowe zasady jego funkcjonowania określa rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej[144]. Zasada neutralności w konsekwencji prowadzi do uznania, iż zarówno sieci jak usługi informacyjne nie powinny być zmonopolizowane. Wskazać nadto należy, iż przepisy prawne pozwalające na wykonywanie władztwa publicznego podmiotowi

[141] Szerzej: A. Monarcha-Matlak, *Wzorce i zasady obecnej i przyszłej administracji publicznej* [w:] B. Jaworska-Dębska (red.), P. Kledzik (red.) J. Sługocki (red.) *Wzorce i zasady działania współczesnej administracji publicznej*, Wolters Kluwer, 2020, s. 908 i nast.
[142] P. Fajgielski, *Informacja w administracji publicznej, prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007, s. 15
[143] J. Blicharz, *W kwestii modelu współczesnej polskiej administracji publicznej,* Przegląd Prawa i Administracji, Tom 77, 2008, s. 35
[144] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. 2007 nr 10 poz. 68)

publicznemu należy postrzegać jako przejaw realizacji nałożonych na niego zadań, które są urzeczywistnieniem interesu publicznego[145].

W Polsce postępowanie administracyjne jest utożsamiane z procedurą załatwiania spraw indywidualnych, podczas gdy przekaz dokumentów elektronicznych nie odbywa się wyłącznie w trybie załatwiania spraw indywidualnych w drodze decyzji administracyjnych[146]. Procedura administracyjna obecnie w bardzo szerokim stopniu wykorzystuje komunikację elektroniczną, gdzie szczególnie pochylić należy się nad udostępnieniem do korzystania dla obywateli z możliwości doręczenia dokumentów drogą elektroniczną oraz elektronicznego potwierdzenia odbioru[147]. Oczywiście, nadal doręczenia metodą tradycyjną to jest za pomocą przedstawiciela pocztowego, wiodą prym i to właśnie te metody należy traktować jako te podstawowe, to jednak komunikacja elektroniczna z pewnością przyspiesza przekazywanie informacji oraz umożliwia ich natychmiastowe przekazanie.

W ramach postępowania administracyjnego, na skutek nowelizacji w związku z ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne, wyczerpująco uregulowano kwestię środków komunikacji elektronicznych[148]. W zakresie celowości ich wprowadzenia, nie ma w zasadzie wątpliwości co do tego, iż zabieg ten miał przede wszystkim przyspieszyć możliwie najbardziej postępowanie przed urzędami, usprawnić je w zakresie doręczeń i podań oraz niejako „otworzyć" działalność organów władzy publicznej na obywateli poprzez ułatwienie do nich dostępu. Nowe przepisy Kodeksu postępowania administracyjnego zapewniają możliwość zrealizowania spraw w urzędach za pomocą komunikacji elektronicznej. Niemniej jednak efektywna e-administracja oraz skuteczność świadczenia e-usług wymaga wdrożenia jednolitych zasad reagowania na ewentualne incydenty o charakterze niebezpiecznym[149].

W ślad za powyżej poczynionymi ustaleniami wskazać należy udostępnienie obywatelom możliwości korzystania z instrumentu w postaci podań wnoszonych za

---

[145] J. Blicharz, *Zakres znaczeniowy pojęcia „zadania publiczne"*, Przegląd Prawa i Administracji, 2005, t. LXXI, s. 66

[146] G. Szpor [w:] *Ustawa o infromatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz, Wolter Kluwer Business*, s. 163

[147] Szerzej: D. Skoczylas, *Aksjologiczny wymiar e-administracji i cyberbezpieczeństwa w kontekście potrzeb jednostki i wspólnoty* [w:] Z. Duniewska (red.), M. Karcz-Kaczmarek (red.), P. Wilczyński (red.), *Prawo administracyjne w służbie jednostki i wspólnoty,* Wolters Kluwer, Warszawa, 2022, s. 207 i nast.

[148] Tak: K. Ziółkowska, *Transformacja administracji w* e-administrację [w:] *Postępowanie administracyjne i sądowoadministracyjne*, red. M. Wierzbowski, Warszawa 2020

[149] Szerzej: D. Skoczylas, *Dynamizm legislacji administracyjnej a cyberbezpieczeństwo i użytkowanie przestrzeni kosmicznej w ramach e-administracji* [w:] M. Kruś (red.), L. Staniszewska (red.), M. Szewczyk (red.) *Kierunki rozwoju jurysdykcji administracyjnej*, Wolters Kluwer, Warszawa 2022, s. 307 i nast.

pośrednictwem dokumentu elektronicznego, które – aby wywołało przewidziane prawem skutki prawne – winno zostać opatrzone bezpiecznym podpisem elektronicznym (przy respektowaniu wymogów prawnych regulujących tę kwestię) oraz być w formacie określonym w odrębnych przepisach, w zależności od przedmiotu załatwienia. Nadto art. 39^1 § 1 k.p.a.[150] ustawodawca przewidział możliwość doręczenia pism przy wykorzystaniu środków komunikacji elektronicznej, jeśli strona wniosła lub wyraziła zgodę na doręczenie w ten sposób. Wyżej przytoczone przepisy to tylko podstawowe regulacje, których konieczne było przywołanie w tym miejscu. Są to podstawowe dyspozycje, obrazujące jedynie postęp rozwoju dostępu do informacji, w tym załatwiania określonych spraw, przy udziale organów administracji publicznej. Kodeks postępowania administracyjnego wyczerpująco reguluje kwestię zarówno wniosków, podań, ale również doręczeń i innego sposobu załatwiania spraw przed urzędami, przy wykorzystaniu środków komunikacji elektronicznej. Kwestia ta jednakże kompleksowo zostanie omówiona w dalszych rozdziałach pracy, z omówieniem wymiaru praktycznego, a także przeprowadzenia badań dotyczących ich rzeczywistego wykorzystania. W związku z potrzebą odtworzenia definicji legalnych podstawowych pojęć, konieczne jest zwrócenie uwagi na problematykę obowiązku ochrony danych osobowych w komunikacji elektronicznej[151]. Kwestia ta również zostanie szczegółowo omówiona w dalszym toku niniejszej pracy, z uwzględnieniem poszczególnych instrumentów, środków komunikacji elektronicznej, a także regulacjami prawnymi oraz analizą czy respektują one szczegółowe zasady dotyczące ochrony danych osobowych.

Przekazywanie, udostępnianie oraz gromadzenie informacji w drodze komunikacji elektronicznej stwarza ogromne i w zasadzie nieograniczone możliwości przetwarzania danych osobowych. Ogromną wadą wykorzystania środków komunikacji elektronicznej jest niebezpieczeństwo utraty danych bądź trafienia ich w nieodpowiednie miejsce. Mając to na względzie wszelkie regulacje prawne, które winny zmierzać do zapewnienia bezpieczeństwa obrotu prawnego, a w konsekwencji bezpieczeństwa danych osobowych, powinny być podejmowane w sposób bardzo przemyślany, w taki sposób, aby zapewnić maksymalną ochronę przekazywanych w drodze komunikacji elektronicznej informacji. Na gruncie prawa Unii Europejskiej podstawowym źródłem ochrony danych pierwotnie była Konwencja Rady Europy nr 108 z dnia 24 października 1981 r. o ochronie osób w związku z automatycznym

[150] Ustawa z dnia 14 czerwca 1960 roku Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775)
[151] Szerzej: J. Mielczarek-Mikołajów, *Ochrona danych osobowych z perspektywy rozwoju e-administracji* [w:] M. Jędrzejczak (red.), *Ochrona danych osobowych w prawie publicznym,* Wolters Kluwer, 2021, s. 49 i nast.

przetwarzaniem danych osobowych[152], a następnie przełomowe rozporządzenie RODO[153]. W polskim porządku prawnym kwestia ta znajduje w pierwszej kolejności oczywiście potwierdzenie w art. 51 Konstytucji zapewniającym ochronę informacji oraz prywatności jak również przepisy szczególne uregulowane w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Ochrona danych osobowych poruszona nadto została na kanwie ustawy o świadczeniu usług drogą elektroniczną oraz ustawy – Prawo telekomunikacyjne.

Powyżej poczynione ustalenia wskazują, iż z uwagi na nowy charakter dziedziny prawa jaką jest prawo komunikacji elektronicznej, istnieje problem zdefiniowania wielu pojęć, których znaczenie należy odtwarzać na podstawie zarówno prawa krajowego jak i prawa unijnego. Ustawy regulowane w ramach porządku krajowego zawierają co prawda definicje legalne niektórych z wyżej przytoczonych pojęć, natomiast dyspozycje zawarte w prawie Unii Europejskiej niejednokrotnie (nie zawsze znacząco) zmieniają i modyfikują przyjęte znaczenie. Reasumując wskazać jednoznacznie należy, iż kwestia prawidłowego zdefiniowania pojęć dla zapewnienia jasności i precyzyjności oraz racjonalności prawodawcy, jak również zapewnienie bezpieczeństwa prawnego, ochronę informacji i danych osobowych w ramach ich przekazywania i gromadzenia, ochrona prywatności – znajduje się w gestii prawodawcy. Nie ma wątpliwości również co do tego, iż komunikacja elektroniczna jest współcześnie czynnikiem podstawowym i decydującym w rozwoju społeczeństwa, a dziedzina prawa komunikacji elektronicznej wraz z postępem technologicznym, będzie nieustannie wymagała modernizacji i reformowania, dla zapewnienia ich skutecznego stosowania oraz bezpieczeństwa obrotu prawnego.

[152] Konwencja Rady Europy nr 108 z dnia 24 października 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, Dz. U. z 2003 r. Nr 3, poz. 25 z późn. zm.
[153] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w s sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1)

Rozdział II

Teoretycznoprawne aspekty funkcjonowania zawodów prawniczych

Problemem badawczym stanowiącym przedmiot niniejszej pracy jest ocena wpływu nowych technologii na funkcjonowanie zawodów prawniczych. W związku z koniecznością analizy tej kwestii nie tylko w odniesieniu do całości grupy zawodowej, ale w również w kontekście konkretnej profesji, analizie poddać należy również teoretycznoprawne uregulowania dotyczące zawodów prawniczych oraz ich funkcjonowania. Sfera szeroko rozumianych zawodów prawniczych jest niezwykle bardzo „narażona" na działanie nowych technologii. Co więcej, nowe technologie opanowując niemalże każdą strefę życia publicznego, w sposób decydujący wpływają również na funkcjonowanie zawodów prawniczych. Nieustannie prosperujące nowe technologie, a nadto wykorzystanie w coraz to większym stopniu środków komunikacji elektronicznej przez zawody prawnicze, na przestrzeni dziejów diametralnie zmieniło sposób ich funkcjonowania nie tylko w społeczeństwie, ale również w obrocie prawnym oraz w relacji z innymi zawodami prawniczymi.

1. Definicja pojęcia „zawody prawnicze"

W pierwszej kolejności należy odnieść się do definicji i znaczenia pojęcia zawody prawnicze, albowiem jest to tak szerokie zagadnienie, że w kontekście przedmiotowej pracy w pełni celowe i uzasadnione jest jego precyzyjne omówienie. Bez wątpienia od lat zawody prawnicze przez społeczeństwo zostały umiejscowione w sferze zawodów zaufania publicznego. Nierozerwalnie związane jest to ze sferą działalności, która odnosi się do kluczowego i najbardziej istotnego pojęcia dla społeczeństwa, tj. sprawiedliwości, która jest najbardziej pożądaną z cnót[154]. Zawody prawnicze w zasadzie od początków ich funkcjonowania utożsamiane były z wyższą klasą społeczną, a nawet elitą, zajmującą się regulacją stosunków między ludźmi. Niejednokrotnie w społeczeństwie tą grupę traktowano jako zamkniętą kastę, do której dostęp mieli wyłącznie członkowie rodziny, w tym potomkowie mieli zapewnioną przyszłość. Uznawano, iż sfera ta jest niemalże niedostępna dla osoby nie mającej wśród swoich przodków prawnika. Granica ta, co zdecydowanie wymaga pozytywnej oceny, z biegiem czasu, rozwoju i chęcią nauki i dostępem do niej, zaczęła być niemal

[154] Szerzej: M. Grześkowiak, *Udział obywateli w sprawowaniu wymiaru sprawiedliwości w państwach demokratycznych,* [w:] R. Piotrowski (red.) *Udział obywateli w sprawowaniu wymiaru sprawiedliwości*, 2021

niewidoczna, do tego stopnia, że współcześnie sfera zawodów prawniczych jest w zasadzie całkowicie otwarta i dostępna dla wszystkich.

Ukończenie studiów prawniczych jest podstawowym kryterium umożliwiającym przyjęcie do grupy zawodów prawniczych. Wówczas uzyskuje się tytuł prawnika zamiennie stosowanego z tytułem magistra prawa, który to zawód umożliwia rozpoczęcie działalności na różnych płaszczyznach, w tym możliwości ubiegania się o dane stanowisko poprzez odbycie aplikacji właściwej dla danego zawodu, której pozytywne ukończenie wraz ze złożeniem egzaminu zawodowego nie każdorazowo oznacza uzyskanie określonego tytułu zawodowego, albowiem niekiedy konieczne jest odbycie dwu- lub trzyletniej asesury, będącej niejako bezpośrednim przygotowaniem do faktycznego wykonywania zawodu, który z racji swojej istoty obciążony jest ogromną odpowiedzialnością.

Niejednokrotnie w doktrynie napotyka się krytyczną ocenę długiej ścieżki naukowej i zawodowej pozwalającej uzyskać konkretny tytuł zawodowy dla prawników. W przypadku organów ścigania oraz zawodów funkcjonujących w sferze wymiaru sprawiedliwości, zwłaszcza sędziów, droga do samodzielnego stanowiska zawodowego jest naprawdę długotrwałą nauką i poważnym procesem budowania doświadczenia zawodowego[155]. Niemniej jednak cała ta materia wydaje się mieć mocne uzasadnienie zarówno logiczne jak i aksjologiczne. Skoro bowiem zawody prawnicze traktowane są jako zawody zaufania publicznego[156], a nadto dotyczą sfery wrażliwej, delikatniej, będącej bardzo blisko zasobów ludzkich i ludzkich potrzeb, w pełni uzasadnione zatem zdaje się być to, iż przygotowanie do wykonywania tej profesji również musi odpowiadać powadze tej działalności, aby możliwie jak najbardziej uniknąć nierzetelnych prawników zajmujących się – w dużym skrócie ujmując – interesem publicznym. Specyfika wykonywanej profesji wymaga zbudowania nie tylko odpowiedniego doświadczenia zawodowego, ale również, a być może nawet przede wszystkim niezbędne jest posiadanie właściwie rozbudowanego doświadczenia życiowego[157]. Niejednokrotnie wskazuje się, iż właśnie doświadczenie zawodowe oraz umiejętność logicznego myślenia i właściwego powiązania faktów jest kluczowa przy podejmowaniu decyzji, zwłaszcza przy orzekaniu[158]. Kwestia ta zostanie również zasygnalizowana przy okazji

[155] Szerzej m.in.: D. Drajewicz, *Kryteria powołania na stanowisko sędziego,* Przegląd Sądowy 2017/2/77-87
[156] Por. Art. 17 ust. 1 Konstytucji Rzeczypospolitej Polskiej, P. Tuleja (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wyd. II*, 2021
[157] T. Kanty, *Doświadczenie życiowe a ocena dowodów w procesie karnym,* Państwo i Prawo 2018/7/23-37
[158] Por. art. 7 ustawy Kodeks postępowania karnego – zasada swobodnej oceny dowodów, J. Kasiński [w:] D. Świecki (red.), *Kodeks postępowania karnego. Orzecznictwo,* Wolters Kluwer, 2022

omawiania profesji sędziego, który to zawód wielokrotnie wskazywany jest jako korona zawodów prawniczych. Niezależnie od powyższego, podejmując rozważania w zakresie działalności prawników nie sposób pominąć niezwykle ważnego aspektu ich działalności, która odróżnia tą profesję od wielu pozostałych. Wspólnym mianownikiem wszystkich zawodów prawniczych jest przyjęcie ich do wąskiej grupy zawodowej jaką są zawody zaufania publicznego[159]. Pojęcie to zostało wprowadzone przez art. 17 Konstytucji Rzeczypospolitej Polskiej, który utożsamia wykonywanie zawodu zaufania publicznego z istnieniem samorządu zawodowego[160]. Przyjmuje się, iż do zawodów zaufania publicznego zalicza się profesje polegające na wykonywaniu działań o szczególnym charakterze z punktu widzenia zadań publicznych i z troski o realizację interesu publicznego[161]. Wielokrotnie, choć nie do końca należy ocenić to pozytywnie, pojęcie zawodów zaufania publicznego zamiennie używa się z pojęciem wolnych zawodów, o których będzie mowa poniżej.

Wśród zawodów prawniczych wyróżnić należy m.in. wolne zawody[162]. Co prawda ustawodawca nie uregulował normatywnej definicji tego pojęcia, niemniej jednak kryterium przyjętym jako spoiwo tej definicji uznać można przynależność (dobrowolna lub zobowiązująca w drodze ustawy) do samorządu zawodowego. Uznać również należy, iż jest to działalność wyposażona w atrybut samodzielności, działania we własnym imieniu i na własny rachunek, w sposób niezależny zawodowo. W literaturze w zasadzie zgodnie przyjmuje się definicję zaproponowaną przez prof. Krystynę Wojtczak, według stanowiska której wolnym zawodem jest osobiste i samodzielne wykonywanie wewnętrznie spójnego zespołu czynności o charakterze intelektualnym[163], wymagających wysokich kwalifikacji, tj. wiedzy i praktyki, systematycznie, w zamian za honorarium bezinteresownie ustalone, służące zapewnieniu świadczeń i usług klientom oraz ochronie istotnych wartości interesu ogólnego, zgodnie z obowiązującymi normami prawnymi, zasadami etycznymi i ontologicznymi[164].

---

[159] Szerzej: P. Sarnecki, *Pojęcie* zawodu zaufania publicznego *(art. 17 ust. 1 Konstytucji na przykładzie adwokatury)* [w:] *Konstytucja. Wybory. Parlament. Studia ofiarowane Zdzisławowi Jaroszowi*, red. L. Garlicki, 2000 oraz M. Tabernacka, *Pojęcie* zawodu zaufania publicznego, AUWr. Przegląd Prawa i Administracji 2004/2663

[160] L. Garlicki (red.), M. Zubik (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom I, wyd. II*, Wyd. Sejmowe, 2016

[161] Opracowania tematyczne, Kancelaria Senatu Biuro Analiz i Dokumentacji, listopad 2013 r., k. 3

[162] J. Jacyszyn, *„Wolny zawód" – anachronizm czy istotne pojęcie prawne?,* Przegląd Prawa Handlowego 2015/11/14-19

[163] K. Wojtczak, *Zawody zaufania publicznego, zawody regulowane oraz wolne zawody. Geneza, funkcjonowanie i aktualne problemy*, Kancelaria Senatu, Biuro Analiz i Dokumentacji, 2013

[164] K. Wojtczak, *Co to jest wolny zawód,* Zeszyty Naukowe WSZiB, 1997, s. 127 i nast.

Poszukując części wspólnej pomiędzy zakresem definicji wolnego zawodu a zakresem definicji zawodów prawniczych, bez wątpienia w pierwszej kolejności wskazać należy grupę, do której przynależą adwokaci i radcowie prawni[165]. W zakresie działalności tych zawodów wskazać należy, iż są to prawnicy świadczący pomoc prawną, w szczególności polegającą na udzielaniu porad prawnych, ale również reprezentowaniu i ochrony interesów przed sądami i innymi instytucjami, w tym państwowymi[166]. W obecnym porządku prawnym możliwe jest omawianie dwóch tych zawodów jednocześnie, albowiem nie wykazują one znaczących różnic z perspektywy przedmiotowych rozważań. W tym stanie rzeczy wskazać należy, iż przed nowelizacją[167] uprawnienia i kompetencje radców prawnych i adwokatów znacznie się różniły, albowiem radcowie prawni specjalizowali się zazwyczaj w prawie handlowym, prawie gospodarczym i w zasadzie pozbawieni byli możliwości występowania w postępowaniu karnym. Po zmianach oraz uzyskaniu przez ten zawód możliwości reprezentowania interesów klientów również w procedurze karnej, różnice w działalności tych zawodów są niemal niedostrzegalne. Niemniej jednak w praktyce przyjęło się, iż radcowie prawni nadal są specjalistami w dziedzinie szeroko rozumianego prawa gospodarczego. Na tle niniejszej pracy zasygnalizować jedynie należy, iż zarówno adwokatem jak i radcą prawnym może być osoba, która pozytywnie złoży egzamin radcowski lub adwokacki po odbyciu 3 letniej aplikacji odpowiednio radcowskiej lub adwokackiej[168]. Prawodawca co prawda w tym zakresie przewiduje nieliczne wyjątki, natomiast na kanwie niniejszych rozważań całość uwagi należy poświęcić na środkach komunikacji elektronicznej oraz nowych technologiach wywierających bezpośredni wpływ na działalność tej grupy zawodowej.

Specyficzną grupę wśród wolnych zawodów, wymagającą odrębnego omówienia z wielu względów jest grupa notariuszy. Analogicznie jak wyżej, notariuszem może co do zasady zostać osoba, która złożyła egzamin notarialny, po uprzednim odbyciu aplikacji notarialnej[169]. Grupa ta wymaga oddzielnej charakteryzacji, albowiem jest to zawód mający nie wiele wspólnego z działalnością adwokatów i radców prawnych, albowiem odnosi się do zupełnie innej strony działalności prawniczej. Za notariusza, dawniej nazywanego rejentem, uznaje się osobę upoważnioną przez władzę państwową do stwierdzenia pewnych faktów i zdarzeń wywołujących skutki prawne oraz osobę, której współdziałanie jest niezbędne przy

[165] Szerzej: J. Jacyszyn, *Wykonywanie wolnych zawodów w Polsce,* Lexis Nexis 2004
[166] K. Wojtczak, *Co to jest* wolny zawód, Zeszyty Naukowe WSZiB 1997, nr 1
[167] Od lipca 2015 roku radcy prawni mogą występować w sprawach karnych z urzędu
[168] Por. art. 24 ust. 1 ustawy z dnia 6 lipca 1982 roku o radcach prawnych (Dz.U. z 2022 r. poz. 1166) oraz art. 65 ustawy z dnia 26 maja 2982 roku Prawo o adwokaturze (Dz.U. z 2022 r. poz. 1184, 1268)
[169] Por. art. 11 ustawy z dnia 14 lutego 1991 roku Prawo o notariacie (Dz. U. z 2022 r. poz. 1799)

sporządzaniu pewnych, upraszczając – aktów prawnych. Zgodnie z dyspozycją art. 1 § 1 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie[170] notariusz jest powołany do dokonywania czynności, którym strony są obowiązane lub pragną nadać formę notarialną. Notariusz nadto w zakresie przysługujących mu uprawnień funkcjonuje w obrocie jako osoba zaufania publicznego, co w konsekwencji oznacza, iż korzysta z ochrony przysługującej funkcjonariuszom publicznym[171]. Charakterystyczną cechą tej grupy zawodowej, jest również fakt, iż notariusza powołuje i wyznacza siedzibę jego kancelarii Minister Sprawiedliwości a także to, że notariusz podczas wykonywania swojej działalności posługuje się pieczęcią urzędową z wizerunkiem orła. Podsumowując istotę zawodu notariusza oraz jego pozycję w polskim systemie prawnym, jednoznacznie wskazać należy, iż w pełni celowe i uzasadnione będzie stwierdzenie, zgodnie z którym notariusz to prawnik pełniący funkcję gwaranta bezpieczeństwa i pewności obrotu prawnego, w kluczowych jego dziedzinach, będącym bezstronnym „doradcą prawnym", który wyposażony jest w atrybut możliwości nadania dokumentom waloru urzędowego[172].

Analogicznie jak przedstawiono powyżej, z podobnych względów, kolejnym elementem działalności prawniczej jest zawód komornika, który nie bez powodu omawiany jest bezpośrednio po zawodzie notariusza, albowiem przejawia on wiele podobieństw zwłaszcza w zakresie statusu społecznego, wykazując jednak zasadnicze różnice w kwestii przysługujących kompetencji. Analogicznie jak w przypadku notariusza, komornikiem może zostać osoba, która – oprócz wskazanych na wstępie wymogów formalnych, które są niezbędne dla wykonywania wszystkich zawodów prawniczych – ukończyła aplikacje komorniczą oraz pomyślnie złożyła egzamin komorniczy, a nadto uprzednio pracowała w charakterze asesora komorniczego co najmniej 2 lata[173]. Wszystkie przywołane wymogi oczywiście są powszechnie przyjętą, odpowiednio uregulowaną zasadą, natomiast ustawodawca przewidział od niej wyjątki dotyczące m.in. sędziów, prokuratorów, adwokatów, radców prawnych czy notariuszy. Komornik sądowy jest funkcjonariuszem publicznym, wykonującym swoją działalność przy właściwym sądzie rejonowym, w skrócie zajmującym się wykonywaniem rozstrzygnięć o roszczeniach cywilnych w drodze przymusu egzekucyjnego. Oczywiście nie jest to wyłączna sfera działalności komornika sądowego, albowiem na mocy ustawy upoważniony on jest również do szeregu innych, równie istotnych czynności m.in. sporządzania na wniosek sądu

[170] Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie (Dz. U. z 2022 r. poz. 1799)
[171] W. Gonet (red.), *Prawo o notariacie. Komentarz,* Wolters Kluwer, 2022
[172] Szerzej: A. Oleszko, *Prawo o notariacie. Komentarz. Tom 1. Ustrój notariatu,* Wolters Kluwer, 2016
[173] Por. Art. 11 ustawy z dnia 22 marca 2018 r. o komornikach sądowych (Dz. U. z 2023 r. poz. 590, 614)

lub prokuratora protokołu stanu faktycznego przed wszczęciem postępowania sądowego lub przed wydaniem orzeczenia. Podstawą prawną wykonywania zawodu komornika jest ustawa z dnia 22 marca 2018 r. o komornikach sądowych[174] oraz ustawa z dnia 28 lutego 2018 r. o kosztach komorniczych[175]. Przy wykonywaniu swojej działalności komornicy wyposażeni są w atrybut niezawisłości i podlegają wyłącznie ustawom, orzeczeniom sądowym oraz prezesowi sądu rejonowego, przy którym prowadzą działalność[176].

2. Środki komunikacji elektronicznej w działalności adwokatów i radców prawnych

W związku z nieustannym rozwojem wykazywanym w sferze komunikacji elektronicznej oraz regularnie rosnącym zainteresowaniem nowymi technologiami również w branży zawodów prawniczych, w działalności adwokatów, ale również radców prawnych od kilku lat można zaobserwować proces informatyzacji[177], który aktualnie znacznie się nasilił. To w pełni zrozumiałe, że adwokatura dąży do popularyzacji nowych technologii wśród adwokatów i w zasadzie nie dotyczy to skomplikowanych i profesjonalnych narzędzi, a podstaw funkcjonowania w komunikacji elektronicznej.

Mimo, iż kilkukrotnie na kanwie niniejszej pracy wskazywano na ten fakt, to jednak warto ponownie podkreślić, iż w zakresie używania narzędzi sprzyjających prawidłowemu funkcjonowaniu komunikacji elektronicznej, decydujące znaczenie mają zabiegi prawodawcze, które niejako wyznaczają szlaki w tym zakresie. Działania ustawodawcze podyktowane są rozwojem nowych technologii i pojawianiem się nowych środków komunikacji elektronicznej, które mają pozytywnie wpłynąć na działalność na wielu płaszczyznach, zwłaszcza poprzez usprawnienie i maksymalne przyspieszenie procedur – zarówno karnych, cywilnych jak i administracyjnych. W tym zakresie niezwykle istotne zdaje się być wprowadzenie nowych rozwiązań prawnych na kanwie ustawy o doręczeniach elektronicznych[178]. Od dnia 1 października 2021 r. adwokaci, radcy prawni, ale również notariusze są zobowiązani do posiadania adresu do doręczeń elektronicznych wpisanego do bazy adresów elektronicznych,

[174] Ustawa z dnia 22 marca 2018 r. o komornikach sądowych (Dz. U. z 2023 r. poz. 590, 614)
[175] Ustawa z dnia 28 lutego 2018 r. o kosztach komorniczych (Dz. U. z 2023 r. poz. 1357)
[176] Szerzej: A. Grajewski, *Art. 11 – kwalifikacje niezbędne przy powołaniu* [w:] M. Simbierowicz (red.), M. Świtkowski (red.), *Komentarz do ustawy o komornikach sądowych. Ustawa o komornikach sądowych. Ustawa o kosztach komorniczych. Komentarz, wyd. III,* Wolters Kluwer, 2023
[177] Szerzej: S. Kotecka-Kral, *Informatyzacja działalności korporacji prawniczych na przykładzie postępowania cywilnego* [w:] K. Flaga-Gieruszyńska (red.), J. Gołaczyński (red.), Prawo Nowych Technologii, Wolters Kluwer, 2021
[178] Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. z 2023 r. poz. 285)

powiązanego z publiczną usługą rejestrowanego doręczenia elektronicznego albo kwalifikowaną usługą rejestrowanego doręczenia elektronicznego. To zdecydowany zwrot w stronę sędziów, dla których będzie to znaczne ułatwienie, albowiem w pierwszej kolejności sądy właśnie na te adresy mogą przesyłać wszelkie pisma procesowe[179]. Pozytywnie należy również ocenić zmianę jaka pojawiła się w I kwartale 2021 r., zgodnie z którą w procedurze cywilnej możliwe jest podanie w piśmie procesowym nie tylko numeru telefonu, ale również adresu poczty elektronicznej strony, przedstawiciela ustawowego lub pełnomocnika. Nie ma wątpliwości co do tego, iż środki sprzyjające komunikowaniu się na odległość pozytywnie wpływają na ekonomikę procesu, ale również zdecydowanie przyspieszają obieg informacji[180]. Niezależnie od powyższego, wszelkie środki komunikacji elektronicznej obok prawidłowo i rzetelnie przygotowanych do tego systemów, wymagają zastosowania instrumentów zapewniających maksymalną ochronę i bezpieczeństwo przekazywanych danych i informacji, zwłaszcza mając na względzie, iż działalność zawodów prawniczych zazwyczaj dotyczy sfery bardzo wrażliwej. W tym miejscu zaznaczyć jedynie należy, iż w tym stanie rzeczy można dostrzec dość poważne niebezpieczeństwo, co jest najbardziej dostrzegalne właśnie w działalności adwokatów i radców prawnych. Wielokrotnie w praktyce spotyka się, iż prawnicy w zakresie wykonywanej przez siebie działalności prawniczej posługują się darmowymi kontami pocztowymi. Administratorzy takich domen internetowych, zapewne z uwagi na bezpłatność usług, zapewniają bardzo niską jakość bezpieczeństwa oraz niską jakość pewności komunikacji. Mając na względzie te okoliczności, tym bardziej pozytywnie należy ocenić zabieg legislacyjny ustawodawcy związany z informatyzacją wymiaru sprawiedliwości a w konsekwencji koniecznością posiadania adresu poczty elektronicznej przez przedstawicieli zawodów prawniczych. Wówczas adresy powinny zostać zgromadzone na jednej platformie, być obsługiwane przez administratora domeny, który zapewni najwyższą jakość usług, zwłaszcza w zakresie poziomu bezpieczeństwa.

2.1. Innowacyjne rozwiązania w pracy notariusza

Mając na uwadze wyżej poczynione ustalenia ponownie zasygnalizować należy, iż nowelizacja dotycząca obowiązkowego posiadania adresu do doręczeń elektronicznego wpisanego do bazy adresów elektronicznych, powiązanego z publiczną usługą rejestrowanego doręczenia elektronicznego albo kwalifikowaną usługą rejestrowanego doręczenia

[179] Szerzej: M. Wilbrandt-Gotowicz (red.), *Doręczenia elektroniczne. Komentarz*, Wolters Kluwer, 2021
[180] Por. wyrok Naczelnego Sądu Administracyjnego z dnia 18 maja 2017 r. sygn. II FSK 454/17

elektronicznego dotyczy również działalności notariuszy. Wielokrotnie przy okazji debat na konferencjach dotyczących wpływu nowych technologii na działalność zawodów prawniczych, ale również w literaturze właściwej dla przedmiotu rozważań wskazuje się na ryzyko i zagrożenie związane z rozwojem technologicznym dla działalności notariusza. Nie ma wątpliwości w zasadzie co do tego, iż pojawienie się oraz rozwój nowych technologii miało ogromny wpływ na działalność kancelarii notarialnych. Zdaniem części doktryny uzasadnione jest to przede wszystkim specyfiką wykonywanej profesji, która w przyszłości, wraz z rozwojem nowych technologii i coraz to większym ich przełożeniem na działalność prawników, może zostać zastąpiona systemami wykorzystującymi sieć teleinformatyczną. Zdaniem przeciwników tej teorii, co zdaje się być bardziej rzeczowe i realne, mimo wszystko zawód notariusza nadal będzie potrzebny, albowiem wiele czynności pomimo zastosowania chociażby najbardziej rozwiniętej sztucznej inteligencji, będzie wymagało czynnika ludzkiego. Słuszne zdaje się być stanowisko, zgodnie z którym praca notariusza bardzo często wymaga potwierdzenia tożsamości klienta, natomiast trudne do wyobrażenia zdaje się być wykonanie tej czynności przez komputer. Działanie takie z pewnością implikowałoby szereg wątpliwości co do rzetelności i rzeczywistego bezpieczeństwa w tym zakresie.

W zakresie profesji notariusza oraz wykorzystywania w jego działalności nowych technologii oraz baz danych wykorzystujących te aspekty, w pierwszej kolejności bez wątpienia wskazać należy na system Rejestrów Notarialnych stworzonych w 2009 r. przez samorząd notarialny. Jest to system teleinformatyczny zbierający i udostępniający dane przetwarzane przez sądy, notariuszy Rzeczpospolitej Polskiej oraz notariuszy Unii Europejskiej[181]. Na przestrzeni lat, systemy te były sukcesywnie modernizowane i rozbudowywane o nowe moduły, zaś za gruntową przemianę przyjmuje się 2016 r. Aktualnie Rejestry Notarialne zawierają:

- Rejestr Użytkowników (m.in. ustawowe listy notariuszy i zastępców notarialnych),
- Rejestr Spadkowy (informacje o zarejestrowanych notarialnych aktach poświadczenia dziedziczenia, sądowych stwierdzeniach nabycia spadku i europejskich poświadczeniach spadkowych),
- Notarialny Rejestr Testamentów,
- Centralne Repozytorium Elektronicznych Wypisów Aktów Notarialnych,
- Rejestr Zarządców Sukcesyjnych przedsiębiorców osób fizycznych,

[181] Ł. Goździaszek, *Informatyzacja postępowania cywilnego* [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, *Prawo nowych technologii*, Wolters Kluwer, 2021, s. 137 i nast.

– Notarialne Rejestry Statystyczne.

Powyżej wspominany system, który może zostać utożsamiany z klasyczną bazą danych, aczkolwiek stanowią nie tylko rejestry, ale również podsystemy wymiany danych z instytucjami zewnętrznymi między innymi z sądami wieczystoksięgowymi[182], Krajowym Rejestrem Sądowym, Ministerstwem Sprawiedliwości, CEIDG, Europejską Siecią Rejestrów Testamentów oraz Europejską Siecią Notarialną. System nadto przewiduje również opcję wyszukiwania pewnych danych, również za pomocą sieci teleinformatycznej. Kwestia gromadzenia i przechowywania danych, w tym ich ochrony oraz podstaw przetwarzania zostanie omówiona w odrębnym rozdziale. W ramach systemu Rejestrów Notarialnych zgodnie z dyspozycją art. 92a ustawy Prawo o notariacie Krajowa Rada Notarialna prowadzi Centralne Repozytorium Elektronicznych Wypisów Aktów Notarialnych (zwany dalej: CREWAN)[183]. Oczywiście, analogicznie jak powyżej, jest on prowadzony w systemie teleinformatycznym, gdzie przechowywane są elektroniczne wpisy i wyciągi z aktów notarialnych, ale sporządzonych wyłącznie na terytorium Rzeczpospolitej Polskiej[184]. Dostęp do systemu CREWAN mają sądy, notariusze oraz inne organy państwowe uprawnione na podstawie przepisów szczególnych[185]. W obecnie obowiązującym porządku prawnym ustawodawca nakłada na notariusza obowiązek umieszczenia elektronicznego wypisu w systemie oraz opatrzenia go kwalifikowanym podpisem elektronicznym niezwłocznie po sporządzeniu aktu notarialnego zawierającego w swej treści dane stanowiące podstawę wpisu do rejestru przedsiębiorców KRS albo podlegającego złożeniu do akt rejestrowych podpisu wpisanego do rejestru przedsiębiorców KRS. Pozostałe wypisy w Repozytorium umieszcza się wówczas, jeśli wynika to wprost z innych przepisów oraz pozwalają na to warunki organizacyjno-techniczne systemu teleinformatycznego[186]. Warto wskazać również, iż informatyzacja działalności notariusza pozwala również na to, że po wprowadzeniu wyżej określonych informacji do systemu, notariusz otrzymuje za pośrednictwem sieci teleinformatycznej zawiadomienie zawierające w swojej treści numer dokumentu w CREWAN, a także dzień, miesiąc i rok oraz

[182] Szerzej o informatyzacji rejestrów publicznych: A. Gryszczyńska, *Nowa Księga Wieczysta. Informatyzacja rejestru publicznego*, Lexis Nexis 2011

[183] Szerzej: Ł. Zamojski, *Krajowy Rejestr Sądowy. Komentarz, wyd. II,* Wolters Kluwer, 2023, s. 250 i nast.

[184] Rozporządzenie Ministra Finansów z dnia 28 lutego 2023 r. w sprawie przechowywania w Centralnym Repozytorium Elektronicznych Wypisów Aktów Notarialnych aktów notarialnych, zarejestrowanych aktów poświadczenia dziedziczenia i zarejestrowanych europejskich poświadczeń spadkowych (Dz. U. 2023 poz. 378)

[185] Szerzej: W. Gonet (red.), *Prawo o notariacie. Komentarz,* Wolters Kluwer, 2022

[186] Por. Art. 92a § 1 ustawy Prawo o notariacie

godzinę i minutę jego umieszczenia, co z kolei dołączane jest do oryginału aktu notarialnego, przy czym jedna kopia zawiadomienia udostępniana jest stronie czynności.

Całokształt przytoczonych okoliczności pozytywnie wpływa na funkcjonowanie zawodowe notariuszy, zwłaszcza w zakresie ułatwienia i przyspieszenia wykonywanych przez nich czynności w ramach działalności swojej kancelarii. Nie ma wątpliwości co do tego, iż środki udostępnione notariuszom działają dzięki możliwościom jakie dostarczają nowe technologie, a ich sprawne i rzetelne funkcjonowanie spowodowane jest środkami technicznymi oraz wykorzystaniem sieci teleinformatycznej. Jednoznacznie stwierdzić należy, iż wywołuje to potężny wpływ na bezpieczeństwo przechowywania niezwykle istotnych dokumentów oraz zapobiega negatywnym konsekwencjom w przypadku ich ewentualnej utraty lub zagubienia. Niezależnie od powyższego, należy również wspomnieć o przeobrażeniach w pracy notariusza dokonanych w związku z panującą na świecie pandemią wirusa SARS-COV-2, albowiem konieczność zrealizowania celów ochrony zdrowia obywateli ustawodawca na kanwie ustaw tzw. Tarcz Antykryzysowych wprowadził rozwiązania ułatwiające pracę m.in. notariuszy poprzez udostępnienie mu możliwości zastąpienia dokumentów urzędów formą elektroniczną, co z kolei znów wskazuje wyraźnie na potęgę nowych technologii oraz szeroki zakres ich wykorzystania. Możliwość ta została wprowadzona art. 31zze ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[187]. Zgodnie z brzmieniem przywołanego przepisu, w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii ogłoszonych w związku z COVID-19, notariusz może wydrukować dokument elektroniczny sporządzony przez podmiot publiczny, opatrzyć go następnie datą pewną, ale wyłącznie w sytuacji, w której dokument ten jest niezbędny do przeprowadzenia czynności notarialnej. Ten zabieg legislacyjny w zdecydowany sposób ułatwił, a niekiedy również w ogóle umożliwił przeprowadzanie i wykonywanie czynności notarialnych, w przypadku których wymagane jest posiadanie określonych dokumentów wydanych przez podmiot publiczny, do którego dostęp w czasach pandemii był znacznie utrudniony i ograniczony, a uzyskanie pewnych dokumentów jest niemal niemożliwe. Podkreślenia wymaga fakt, iż rozwiązanie to obowiązuje wyłącznie w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii ogłoszonych w związku z COVID-19, niemniej jednak słusznie wskazuje się, iż takie rozwiązanie zostanie przyjęte również w innych

[187] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2023 r. poz. 1327)

okolicznościach. Na potrzeby przedmiotowych rozważań wskazać należy, iż dokument elektroniczny oznacza stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych, czyli materiale lub urządzeniu służącym do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej[188]. Procedura w tym zakresie przedstawia się następująco. W pierwszej kolejności osoba zainteresowana uzyskaniem dokumentu urzędowego zwraca się do właściwego podmiotu publicznego, aby dostarczył go notariuszowi za pomocą elektronicznej platformy usług administracji publicznej. Następnie notariusz drukuje otrzymany dokument, opatruje go datą pewną, dzięki czemu zyskuje on moc dokumentu urzędowego. Dokument taki stanowi zazwyczaj załącznik do aktu notarialnego. W zakresie praktycznego wykorzystania wskazać należy, iż ma to zastosowanie m.in. w odniesieniu do aktu zgonu spadkodawcy w przypadku aktu poświadczenia dziedziczenia, zaświadczenia o braku zaległości w opłatach z tytułu podatku od nieruchomości w przypadku sprzedaży lub darowizny lokalu mieszkalnego i wiele innych. Mając na względzie powyższe ustalenia, podkreślić należy pozytywny wymiar wprowadzenia takiej regulacji, albowiem nie tylko w czasie obowiązywania pandemii jest to zdecydowane ułatwienie w procesie dokonywania czynności notarialnych. Ten zabieg jako kolejny pokazuje, iż rozwój nowych technologii w sposób znaczący ułatwia funkcjonowanie w wielu sferach życia społecznego.

2.2 Komunikacja elektroniczna w zawodzie komornika

W działalności komorników dostrzega się najmniej spektakularne rozwiązania w zakresie wykorzystania nowych technologii oraz baz danych wykorzystujących system teleinformatyczny, niemniej jednak kwestia posiadania adresu poczty elektronicznej w odpowiedniej domenie, jak w przypadku wyżej omówionych profesji, znajduje zastosowanie również do komorników. Na potrzeby przedmiotowej pracy wskazać należy, iż zgodnie z procedurą cywilną komornik dokonuje doręczeń administracyjnym organom egzekucyjnym, organom podatkowym oraz wierzycielom należności pieniężnych, których egzekucja została przejęta przez sądowy organ egzekucyjny w wyniku zbiegu egzekucji administracyjnej i sądowej, będącym podmiotami publicznymi obowiązanymi do udostępniania i obsługi

[188] A. Skóra *Art. 47 Obowiązki operatora wyznaczonego w zakresie realizacji publicznej usługi hybrydowej; moc dowodowa wydruku dokumentu elektronicznego w ramach publicznej usługi hybrydowej* [w:] B. Kwiatek (red.), A. Skóra (red.), *Doręczenia elektroniczne. Komentarz*, Wolters Kluwer, 2023

elektronicznej skrzynki podawczej, wyłącznie za pośrednictwem systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznych.

3. Wymiar sprawiedliwości – zagadnienia teoretycznoprawne

Kolejną grupą zawodową wymagającą analizy w związku z przedmiotowymi rozważaniami jest grupa zawodowa jaką stanowi wymiar sprawiedliwości, a w zasadzie jego część, tj. sędziowie. Pojęcie „wymiar sprawiedliwości" pochodzi z języka łacińskiego, gdzie *ius dicere* oznacza orzekanie prawa. Zgodnie ze znaczeniem przytoczonym przez encyklopedię PWN należy przez to rozumieć działalność państwa, która jest realizowana przez niezawisłe sądy, które w formie procesowej rozstrzygają konflikty prawne[189]. Zgodnie z Konstytucją RP wymiar sprawiedliwości sprawują Sąd Najwyższy, sądy powszechne (apelacyjne, okręgowe, rejonowe), sądy administracyjne (Naczelny Sąd Administracyjny, wojewódzkie sądy administracyjne) oraz sądy wojskowe[190]. Z uwagi na to, że wymiar sprawiedliwości jest nieodzownym elementem systemów państwowych, a zdaniem wielu – jego fundamentem, na przestrzeni dziejów – ilekroć modyfikacjom ulegał system czy obowiązujący ustrój, implikowało to również konieczność dokonania przeobrażeń w tej sferze, zwłaszcza poprzez przyznawanie na przestrzeni dziejów kolejnych przymiotów[191]. Zmiany te dotyczyły również „ucywilizowania" w tym zakresie, udostępniając sędziom nowe technologie mające na celu usprawnienie i możliwe przyspieszenie procedur, przy jednoczesnym zachowaniu istoty tego zawodu.

Na wstępie przywołać należy warunki formalne jakie ustawodawca nakłada na osobę ubiegającą się o stanowisko sędziego. Zgodnie z obecnie obowiązującymi regulacjami prawnymi sędzią może zostać wyłącznie osoba z odpowiednim wykształceniem, tj. aplikant sędziowski, referendarz sądowy, asystent sędziego, prokurator, adwokat, radca prawny, notariusz, radca prokuratorii generalnej, profesor lub doktor habilitowany nauk prawnych. Nadto kandydat na sędziego musi oczywiście posiadać obok wykształcenia prawniczego, oświadczenie zawodowe, oraz zdać odpowiedni egzamin i mieć ukończone 29 lat[192]. Obecnie aplikacja sędziowska organizowana jest włącznie przez Krajową Szkołę Sądownictwa

[189] Encyklopedia PWN, https://encyklopedia.pwn.pl/szukaj/wymiar%20sprawiedliwości.html (dostęp: 15.03.2023 r.)
[190] Por. Art. 175 Konstytucji Rzeczypospolitej Polskiej, szerzej: P. Tuleja (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wyd. II*, 2021
[191] B. Stępień-Załucka, *Sprawowanie wymiaru sprawiedliwości przez Sąd Najwyższy w Polsce*, Warszawa 2016, s. 1
[192] Por. art. 61 § 1 ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2023 r. poz. 217, poz. 289, 614, 1030).

i Prokuratury z siedzibą Krakowie, a nie jak uprzednio poprzez poszczególne apelacje sądowe. Obowiązujący model dotarcia kandydatów na stanowisko sędziego, wielokrotnie spotyka się z krytyką wśród specjalistów i budzi wiele wątpliwości i zastrzeżeń, zwłaszcza z punktu widzenia wieku kandydatów na sędziów. Przeciwnicy podnosili, iż wiek 29 lat jest niewystarczający z perspektywy doświadczenia zawodowego i życiowego. Oczywiście, idealnym systemem byłby taki, w którym sędziami zostaliby wyłącznie najlepsi z najlepszych prawników, którzy wspaniale sprawdzili się na egzaminach teoretycznych i jeszcze lepiej poradzą sobie w codziennej pracy zawodowej. Niemniej jednak, z pełną świadomością stwierdzić należy, iż taki model jest niemożliwy, niezależnie od wprowadzonych zmian ustawodawczych i ustrojowych.

Zgodnie z Konstytucją Rzeczpospolitej Polskiej w Polsce obowiązuje trójpodział władzy, przy czym jest to władza ustawodawcza, wykonawcza oraz sądownicza. Jak powszechnie wiadomo, władza sądownicza – w znacznym uproszczeniu mówiąc – należy do sędziów. Gdyby konieczne było sformułowanie w jednym zdaniu kompetencji sędziów, wskazać wówczas należałoby, iż są to prawnicy, którzy stoją na straży praworządności i sprawiedliwości, w zakresie zadań których znajdują się najistotniejsze sprawy obywateli, zaś ich działanie w pełni musi odpowiadać prawu. Niejednokrotnie zarówno w doktrynie jak i na konferencjach naukowych podnosi się stanowisko, iż urząd sędziego jest koroną zawodów prawniczych[193]. Teza ta spotyka się zarówno z aprobatą, jak również wieloma krytykami, którzy uważają, że urząd sędziego nie jest w zasadzie niczym „wyjątkowym", odróżniającym się od zawodu chociażby notariusza czy prokuratora. Niemniej jednak za powagą i doniosłością urzędu sędziego przemawia chociażby to, iż w większości państw europejskich sędziowie są powoływani na czas nieokreślony. Instytucja sędziego „na próbę" istnieje w zasadzie tylko w ustroju niemieckim, który przewiduje pierwsze powołanie na czas oznaczony do 5 lat[194]. Podkreślić wyraźnie nadto należy, iż z orzecznictwa Europejskiego Trybunału Praw Człowieka w Strasburgu na ustawodawcę krajowego nałożony został obowiązek wyposażenia sądów i sędziów w przymiot niezależności, niezawisłości i bezstronności[195]. Przymiotów tych oczywiście nikt nie kwestionuje, albowiem jest to fundamentalna zasada prawidłowego

[193] Szerzej: Cz. Jaworski, *Urząd sędziego koroną zawodów prawniczych?* [w:] P. Hofmański (red.) *Fiat iustita pereat mundus. Księga jubileuszowa poświęcona Sędziemu Sądu Najwyższego Stanisławowi Zabłockiemu z okazji 40-lecia prawcy zawodowej,* Lexis Nexis 2014 oraz B. Godlewska-Michalak (red.), *Urząd sędziego* koroną zawodów prawniczych*. Materiały pokonferencyjne, Warszawa, 22 kwietnia 2008 r.*, Warszawa 2008

[194] E. Stryczyńska, Urząd sędziego koroną zawodów prawniczych, Krajowa Rada Sądownictwa. 1689-5088. Nr 1, 2008, s. 69-71

[195] J. Barcik, *Niezawisłość sędziowska jako wartość konstytucyjna Unii Europejskiej. Glosa do wyroku Trybunału Sprawiedliwości z dnia 27 lutego 2018 roku, C 64/16,* 2018

funkcjonowania szeroko rozumianej władzy sądowniczej. Wyposażenie jej w takie atrybuty zapewnia realizację w możliwie największym stopniu swoich obowiązków, przy jednoczesnym poszanowaniu godności człowieka i obywatela, ale również tego urzędu. Niezawisłe sądy w istotny sposób przyczyniają się do należytego funkcjonowania demokratycznego państwa prawa, co wynika bezpośrednio m.in. z gwarancji konstytucyjnej, zgodnie z treścią której każdy obywatel ma prawo do rozpatrzenia jego sprawy przez niezależny sąd w rozsądnym terminie[196].

Nie ma w zasadzie wątpliwości do tego, iż działalność sędziego w ramach wykonywanego przez niego zawodu niesie ze sobą najdalej idące konsekwencje w zakresie praw i obowiązków obywatela, a to poprzez wydawanie orzeczeń, które są wiążące. O ile działalność adwokatów czy radców prawnych niewątpliwie niejednokrotnie przyczynia się do ochrony interesów prywatnych, o tyle działalność orzecznicza sędziów bezpośrednio dotyczy sfery najbliższej człowiekowi. Z tego też m.in. powodu urząd sędziego sprawować winna wyłącznie osoba o nieprzeciętnej wiedzy prawniczej, posiadająca nie tylko odpowiednio rozwinięte doświadczenie zawodowe, ale również niezbędne z punktu widzenia orzekania i oceny chociażby materiału dowodowego i okoliczności faktycznych – doświadczenie życiowe. Dlatego też w doktrynie wielokrotnie podnosi się model, zgodnie z którym dojście do zawodu sędziego możliwe było wyłącznie poprzez inne zawody prawnicze. Niemniej jednak model ten wymagałby wprowadzenia szeregu zmian ustrojowych, zapewniających niezwykłą atrakcyjność tego zawodu nie tylko z punktu widzenia prestiżu i godności urzędu, ale również patrząc przez pryzmat wynagrodzenia. W tym miejscu należy przywołać istotny w tym zakresie art. 178 ust. 2 Konstytucji RP, zgodnie z którym sędziom zapewnia się warunki pracy i wynagrodzenie odpowiadające godności urzędu oraz zakresowi ich obowiązków[197]. Nadto trudne byłoby określenie czasu funkcjonowania w danym zawodzie prawniczym, albowiem wiedza prawnicza i zdobywanie doświadczenia życiowego, przy uwzględnieniu różnych zawodów prawniczych a także różnego podejścia to pracy, z pewnością jawiłoby się niejednokrotnie jako niesprawiedliwie lub zbyt długo- albo krótkotrwałe. Ewentualnym rozwiązaniem w tym względzie byłoby zastosowanie cezury wieku, a to z punktu widzenia doświadczenia życiowego, które – jak wyżej wielokrotnie podkreślano – jest jednym z fundamentów pracy sędziego.

Niezależnie od powyższego, podkreślić należy, iż obecny model nie może zostać oceniony jako wadliwy z punktu widzenia dojścia do zawodu sędziego. Pamiętać należy

[196] B. Wagner, *Nieskazitelność charakteru sędziego,* Przegląd Sądowy 2019/11-1/7-18
[197] Szerzej: M. Haczkowska (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz.,* Lexis Nexis 2014

o konieczności odbycia wpierw aplikacji, a następnie podjęcia pracy w ramach asesury sądowej, który to okres ma na celu przygotowanie do zawodu na bardzo wysokim poziomie merytorycznym, ale również kształtowanie postaw wewnętrznej niezależności[198] i nieskazitelności moralnej[199] – niezbędnej wśród sędziów. Wyżej wskazane okoliczności jednoznacznie wskazują, iż okres dotarcia do zawodu sędziego mimo wszystko nie jest krótki i pozwala na zdobycie kwalifikacji uprawniających do wykonywania tego zawodu, albowiem trzy lata aplikacji sędziowskiej, w ramach której odbywa się praktyki w szerokim wachlarzu instytucji państwowych i nie tylko oraz trzy lata asesury są wystarczające co do zasady do przygotowania do sprawowania urzędu sędziego.

3.1. Nowe technologie wykorzystywane przez wymiar sprawiedliwości

Powyżej bardzo szeroko rozważano kwestię zawodu sędziego jako „korony zawodów prawniczych", precyzyjnie i możliwie najdokładniej na potrzeby przedmiotowej rozprawy omówiono zagadnienia dotyczące profesji zawodu sędziego Nie pozostawia wątpliwości teza, zgodnie z którą czynności sędziego wywołują najdonioślejsze skutki w sferach bezpośrednio dotyczących obywateli. Mając to na względzie, środki komunikacji elektronicznej wykorzystywane w profesji sędziów muszą być odpowiednio dobrane, sukcesywnie modyfikowane i nowelizowane na potrzeby społeczeństwa oraz oczywiście objęte szczególną ochroną. Nieustanny rozwój technologiczny oczywiście implikuje konieczność wprowadzenia pewnych przeobrażeń we wszystkich sferach życia społecznego, w tym również w funkcjonowaniu zawodów prawniczych, można zaryzykować stwierdzeniem, iż zwłaszcza w działalności zawodu sędziego. Naczelną zasadą przyświecającą informatyzacji działalności sądów w szerokim ujęciu tego sformułowania, jest maksymalne uproszczenie i przyspieszenie postępowania sądowego, jak również możliwie najbardziej zbliżenie instytucji sądu do obywatela, co z kolei ma gwarantować konstytucyjną zasadę prawa dostępu do sądu oraz do rzetelnego procesu. Nie ma wątpliwości co do tego, iż nie da się wprowadzić jednolitych regulacji w tym zakresie niejako na zawsze, albowiem postęp technologiczny oraz nieustannie pojawiające się nowe rozwiązania implikują konieczność nowelizowania dotychczas obowiązujących regulacji celem regularnego udoskonalania tej właśnie sfery.

[198] Szerzej: J. Sobczak, *Niezawisłość sędziowska i niezależność sądów. Problem ważny i ciągle aktualny,* Gdańskie Studia Prawnicze Przegląd Orzecznictwa 2015/4/79-115
[199] Por. wyrok Sądu Najwyższego z dnia 23 marca 2022 r. sygn. I NKRS 18/22

Obecnie panująca sytuacja na świecie w obliczu pandemii wirusa SARS-COV-2 spowodowała powstanie idealnych warunków nie tylko dla rozwoju nowych technologii oraz dokonywania przeobrażeń w związku z tym w różnych sferach, ale również doskonałych warunków dla wprowadzenia ich do szeregu instytucji oraz zinformatyzowania działalności różnych zawodów, w tym oczywiście również zawodów prawniczych. Uprzednio uznawane za nierealne i niewyobrażalne rozwiązania, aktualnie stały się codziennością, z uwagi na konieczność podejmowania pewnych decyzji na odległość, z wykorzystaniem sieci teleinformatycznej celem zapewnienia maksymalnej ochrony zdrowia zarówno pracowników pewnych instytucji jak również potencjalnych ich „klientów". Instrumentem budzącym największe wątpliwości, ale też jednocześnie trudności organizacyjne oraz techniczne jest wprowadzenie przez ustawodawcę rozpraw sądowych prowadzonych w formie zdalnej[200]. W największym uproszczeniu mówiąc, jest to rozprawa prowadzona za pomocą środków komunikacji elektronicznej, za pomocą urządzeń umożliwiających właśnie tą komunikację na odległość, przy wykorzystaniu sieci teleinformatycznej, gdzie po jednej stronie znajduje się sąd zaś po drugiej strony postępowania oraz ich ewentualni profesjonalni pełnomocnicy czy obrońcy[201]. Na potrzeby zagadnień ogólnych omawianych na kanwie tego rozdziału, zasygnalizować jedynie należy podstawowe zagadnienia związanie w e-rozprawami, albowiem szczegółowo zostanie ona omówiona w odrębnym rozdziale, zwłaszcza w zakresie praktycznego jej zastosowania oraz oceny prawnej wprowadzenia takiego narzędzia. Wobec tego podkreślić należy, iż na mocy ustawy tarcza 3.0 zostały dodane do specustawy art. 15zzs^1 oraz art. 15zzs^4 wprowadzające do postępowania cywilnego oraz sądowoadministracyjnego e-rozprawę lub posiedzenie jawne, które są przeprowadzane przy użyciu urządzeń technicznych umożliwiających przeprowadzenie ich na odległość z jednoczesnym bezpośrednim przekazem obrazu i dźwięku. Ustawa tarcza 3.0 ten sposób procedowania ustanowiła jako zasadę, zaś rozprawy i posiedzenia jawne przy bezpośrednim udziale i obecności stron, pełnomocników i świadków mogą odbywać się jedynie wyjątkowo. Nie ma wątpliwości co do tego, iż wprowadzenie przez ustawodawcę takiego rozwiązania wymaga szeregu rozwiązań technicznych oraz teleinformatycznych, zapewniających prawidłowe i bez zakłóceń procedowanie, ale również – a nawet przede wszystkim – bezpieczeństwo wykonywanych

[200] Por. art. 15zzs ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2023 r. poz. 1327)

[201] M. Kwietko-Bębnowski, *Informatyzacja sądów administracyjnych – próba oceny i poradnik praktyczny,* Przegląd Podatkowy 2020/6/42-48

czynności[202]. Oczywiście e-rozprawy w pełni wykorzystują właściwie rozwiniętą sieć teleinformatyczną, dzięki której możliwie jest prowadzenie rozpraw i posiedzeń jawnych w trybie zdalnym.

W zakresie postępowań karnych będących na etapie sądowym wskazać należy, iż dotychczas ustawodawca przewidywał już wykorzystanie nowych technologii oraz komunikacji elektronicznej, są to m.in. przesłuchanie świadka w trybie art. 177 § 1a k.p.k., przesłuchanie świadka incognito w trybie art. 184 § 4 k.p.k.[203], przesłuchanie świadków w bezpiecznym pokoju z wykorzystaniem środków komunikacji zdalnej na podstawie art. 185a-185c k.p.k. i inne. Jednakże w dodanych § 3 – 9 na mocy art. 39 pkt 8 ustawy nowelizującej z dnia 19 czerwca 2020 r. do art. 374 k.p.k. ustawodawca, niejako na wzór regulacji przyjętych w kodeksie postępowania cywilnego, przewidział rozwiązania umożliwiające udział niektórych stron w rozprawie na etapie postępowania sądowego przy użyciu urządzeń technicznych umożliwiających udział w tych czynnościach na odległość z jednoczesnym bezpośrednim przekazem obrazu i dźwięku. Aspekty praktyczne oraz techniczne związane z tą kwestią zostaną omówione przy okazji omawiania informatyzacji sądów.

Jednoznacznie zasygnalizować trzeba, iż wprowadzenie obowiązku posiadania przez adwokatów czy radców prawnych adresu do doręczeń elektronicznego wpisanego do bazy adresów elektronicznych, powiązanego z publiczną usługą rejestrowanego doręczenia elektronicznego albo kwalifikowaną usługą rejestrowanego doręczenia elektronicznego wywiera bezpośrednie skutki również na działalność sądów, który wówczas musi mieć zdolność do otrzymywania i obsługiwania takich wiadomości. Niezwykle nowatorskim jak na dotychczasowe rozwiązania obowiązujące w krajowym porządku prawnym, jest wprowadzenie przez ustawodawcę systemu tzw. e-doręczeń, które – jak sama nazwa wskazuje – wykorzystują środki komunikacji elektronicznej dla swojego funkcjonowania i skuteczności[204]. W zasadzie zgodnie w literaturze przyjmuje się, iż wprowadzenie takiego modelu doręczeń przez ustawodawcę podyktowane było rozprzestrzeniającą się w kraju i na świecie pandemią koronawirusa, która niejako wymuszała komunikowanie się na odległość. Nie ma wątpliwości

[202] Szerzej: K. Jasińska, *E-rozprawa w postępowaniu cywilnym a możliwość obrony swych praw w kontekście problemów z jej przeprowadzeniem* [w:] B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), *Prawo sztucznej inteligencji i nowych technologii 2*, Wolters Kluwer, Warszawa 2022

[203] Ustawa z dnia 6 czerwca 1997 roku Kodeks postępowania karnego (Dz.U. z 2022 r. poz. 1375, 1855, 2582, 2600, z 2023 r. poz. 289, 535, 818)

[204] Szerzej: M. Wilbrandt-Gotowicz (red.), *Doręczenia elektroniczne. Komentarz*, Wolters Kluwer, 2021

co do tego, iż kwestia doręczeń oraz prawidłowości w tym zakresie ma niebywałe znaczenie dla prawidłowego toku postępowania, w tym również, aby to postępowanie zostało skutecznie wszczęte oraz doszło do rzetelnego merytorycznego zakończenia danej sprawy. Nowe rozwiązania wprowadzone przez ustawodawcę dotyczą tylko specyficznego rodzaju pism procesowych, tj. pozwów (także doręczanych wraz z nakazem zapłaty) oraz innych pism procesowych wywołujących potrzebę podjęcia obrony praw – w zakresie postępowania cywilnego. Jak wyżej wielokrotnie podkreślano, nie ma wątpliwości zarówno co do tego, iż bezpośrednio zabieg taki wpływa na sprawność i przebieg postępowania, ale również co do wątpliwości powstających na kanwie tego zagadnienia zwłaszcza w zakresie bezpieczeństwa jak i wątpliwości co do właściwego czasu zapoznania się z korespondencją oraz jej faktycznego doręczenia. Niemniej jednak kwestia ta zostanie precyzyjnie omówiona na tle kolejnego rozdziału, przy okazji omawiania zagadnień związanych z praktycznymi aspektami wykorzystania nowych technologii przez Sąd.

Podobnie jak w przypadku organów ścigania, sędziowie również mają w zasadzie nieograniczony dostęp do różnego rodzaju baz danych, natomiast na kanwie przedmiotowej pracy nie mają one zasadniczego znaczenia jak w przypadku organów ścigania, gdzie systemy te wykorzystywane są do ścigania przestępstw i ich sprawców. Niemniej jednak dobrze rozwiniętą i regularnie udoskonalaną platformą jest system orzeczeń sądowych umożliwiający dostęp do wokand, orzeczeń oraz przebiegu rozpraw przy wykorzystaniu sieci teleinformatycznej. Działalność sądów w tym zakresie jest dość wysoko zinformatyzowana i umożliwia dostęp do orzeczeń bez udziału w rozprawach czy posiedzeniach sądu, w tym również np. oskarżycielowi publicznemu, który po wylegitymowaniu się odpowiednimi danymi ma nieograniczony dostęp do przebiegu prowadzonych z jego udziałem postępowań zarówno karnych, cywilnych jak i administracyjnych.

4. Organy ścigania – zagadnienia ogólne

Pojęciem „organy ścigania” ustawodawca wielokrotnie posługuje się na tle różnych aktów normatywnych, niemniej jednak dla celów przedmiotowych rozważań w pierwszej kolejności należy przytoczyć ogólne, w zasadzie powszechnie przyjęte znaczenie tego pojęcia. Organy ścigania to organy, do których właściwości należy wykrywanie przestępstw i ściganie ich sprawców poprzez prowadzenie postępowań karnych, a ściślej mówiąc postępowania przygotowawczego, które może być prowadzone w formie śledztwa lub dochodzenia. Fundamentalnymi organami ścigania w Polsce jest prokuratura i Policja. Oprócz nich do

kategorii tej zalicza się Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne, Agencję Bezpieczeństwa Wewnętrznego, Straż Graniczną oraz Służbę Celną.

Biorąc pod uwagę, iż w zakresie wykrywania przestępstw oraz ścigania ich sprawców decydującą rolę odgrywa prokurator a na jego polecenie również funkcjonariusz Policji – na jego działalności skupiona będzie ta część rozważań. W związku z tym na potrzeby niniejszej pracy, ilekroć będzie mowa o organach ścigania uznać należy, iż chodzi właśnie o działalność prokuratora. Na poparcie powyżej wskazanych okoliczności wskazać należy, iż właśnie w ramach funkcjonowania tego zawodu prawniczego udostępniono najszerszy katalog nowych technologii, środków komunikacji elektronicznej, które w czasach postępującej cyberprzestępczości oraz przestępstw popełnianych przy wykorzystaniu urządzeń elektronicznych, są kluczowe z punktu widzenia wykrywania przestępstw oraz ewentualnego zapobiegania ich popełnianiu.

Strukturę prokuratury stanowią Prokurator Generalny, którego urząd sprawuje Minister Sprawiedliwości oraz Prokurator Krajowy, pozostali zastępcy Prokuratora Generalnego oraz prokuratorzy powszechnych jednostek organizacyjnych prokuratury i prokuratorzy Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu[205]. W zasadzie powszechnie przyjmuje się, iż najważniejszym celem funkcjonowania prokuratury jest stanie na straży praworządności oraz ściganie przestępstw[206]. W tym celu prokuratorzy prowadzą i nadzorują postępowania przygotowawcze w sprawach karnych, a w konsekwencji pełnią istotną rolę oskarżyciela publicznego przed sądami. Nadto prokuratorzy sprawują nadzór w sprawach pozakarnych, w tym biorą udział w postępowaniu w sprawach z udziałem osób nieletnich przeprowadzanych na podstawie ustawy o postępowaniu w sprawach nieletnich, ale również podejmują czynności w sprawach cywilnych, chociażby poprzez badanie podstaw do pozbawienia władzy rodzicielskiej, czy też ubezwłasnowolnienia. W zakresie kompetencji prokuratora znajduje się również prawo do zaskarżania do sądu niezgodnych z prawem decyzji administracyjnych, jak również branie udziału w postępowaniu sądowym w sprawach zgodności z prawem takich decyzji, a nadto badanie legalności wydawania aktów prawa miejscowego. Całokształt przytoczonych kompetencji prokuratora jest jedynie ogólnym przytoczeniem najważniejszych aspektów ich działalności, który w rzeczywistości oczywiście jest znacznie szerszy i bardziej szczegółowy[207]. Niemniej jednak ewidentnie pokazuje jak

[205] Por. Art. 1 ustawy z dnia 28 stycznia 2016 r. Prawo o prokuraturze (Dz. U. z 2023 r. poz. 240)
[206] Por. Art. 2 i art. 3 ustawy z dnia 28 stycznia 2016 r. Prawo o prokuraturze (Dz. U. z 2023 r. poz. 240)
[207] Szerzej: P. Turek, *Prawo o prokuraturze. Komentarz.*, Wolters Kluwer, 2023

szerokie uprawnienia znajdują się w zasięgu działania tego zawodu prawniczego, nie jest to zatem zaskakujące, iż jego działalność wspierana i wspomagana jest przez szereg instrumentów, zwłaszcza takich, które w swoim funkcjonowaniu wykorzystują nowe technologie.

4.1. Teleinformatyczne bazy danych wykorzystywane przez organy ścigania

W pierwszej kolejności jednoznacznie zaznaczyć należy, iż działalność prokuratorów w zakresie ścigania przestępstw oraz wykrywania ich sprawców w dużym zakresie wspierana jest przez działania Policji, którzy również w zakresie swoich uprawnień mają możliwość prowadzenia postępowań przygotowawczych prowadzonych w formie dochodzenia. Niemniej jednak istnieje również prawna regulacja, zgodnie z którą, nawet w śledztwach własnych wykonanie czynności procesowych prokurator może zlecić funkcjonariuszom Policji[208]. Oczywiście w tym zakresie ustawodawca przewidział pewne zastrzeżenia, co jest zrozumiałym zabiegiem, albowiem pewne czynności procesowe, zwłaszcza w śledztwie mogą być wykonane wyłącznie przez prokuratora, np. ogłoszenie postanowienia o przedstawieniu zarzutów podejrzanemu[209]. Wraz z postępem technologicznym oraz znacznym wzrostem zainteresowania usługami oferowanymi przez Internet, ale również ujawnioną na początku XXI wieku potrzebą komunikacji międzyludzkiej za pomocą sieci teleinformatycznej, widoczne jest przejście do tego medium czynów zabronionych. Jak wyżej już wskazywano, przestępstwa popełniane za pośrednictwem Internetu określa się mianem cyberprzestępczości, zaś ich sprawców cyberprzestępcami. Łatwy, w zasadzie nielimitowany dostęp do Internetu z niemalże każdego miejsca na ziemi, łatwość nawiązywania kontaktów za jego pośrednictwem, nieustająco wzrastającą popularność, ale również poczucie pozornej anonimowości sprawia, że dane statystyczne w zakresie cyberprzestępczości są zatrważające i wyraźnie wskazują w tym zakresie niezwykle dynamiczną tendencję wzrostową. Ściganie cyberprzestępstw oraz wykrywanie ich sprawców nakłada w związku z tym na organy ścigania ogromne wyzwania i konieczność zmierzenia się z technologiami informatycznymi[210]. W związku z czym dla tego rodzaju spraw udostępniono szereg innych metod związanych z procesem wykrywczym, który oprócz niezwykłej precyzji w działaniu wymaga również podjęcia czynności w odpowiednim czasie z uwagi na retencję danych telekomunikacyjnych, o której będzie mowa w kolejnym

[208] Por. Art. 311 § 2 k.p.k., K. Dudka (red.), *Kodeks postępowania karnego. Komentarz,* Wolters Kluwer, 2020
[209] Por. Art. 311 § 3 k.p.k.
[210] Por. A. Gryszczyńska, *Nowe zagrożenia bezpieczeństwa rejestrów publicznych*, [w:] G. Szpor (red.), A. Gryszczyńska (red.) Internet. Strategie bezpieczeństwa, Warszawa 2017, s. 300–301

rozdziale. Cechą charakterystyczną cyberprzestępstw jest to, że wszelkie jego ślady, tak samo jak środki umożliwiające jego popełnienie w znacznej większości są wirtualne.

Również, a nawet można zaryzykować stwierdzeniem, iż przede wszystkim w zakresie środków komunikacji elektronicznej oraz nowych technologii wsparcie funkcjonariuszy Policji jest nieocenione, albowiem posiadają oni bezpośredni dostęp do baz danych umożliwiających na podstawie bazowych informacji, uzyskać dane bardziej szczegółowe i konkretne. Niejednokrotnie te podstawy finalnie przyczyniają się pośrednio lub bezpośrednio do wykrycia sprawcy przestępstwa. Albowiem na podstawie baz danych możliwe jest wytypowanie kolejnych informacji, a na ich podstawie kolejnych, co w konsekwencji doprowadza do sprawcy czynu zabronionego. Jak wskazano, w zdecydowanej części przypadków organem prowadzącym postępowanie przygotowawcze jest Policja, zaś nadzorującym jest prokurator. Podstawowym systemem wykorzystującym funkcjonowanie nowych technologii opartym na systemie informatycznym jest Krajowy System Informatyczny Policji (zwany dalej KSIP). Najprościej ujmując jest to baza danych pozwalająca na gromadzenie, przetwarzanie i uzyskiwanie informacji kryminalnych[211]. Zgodnie z art. 21nb ust. 1 ustawy o Policji[212] Komendant Główny Policji prowadzi Krajowy System Informacyjny Policji, zwany dalej „KSIP", będący zestawem zbiorów danych, w którym przetwarza się informacje, w tym dane osobowe, w związku z realizacją zadań ustawowych[213]. Administratorem danych, zgodnie z art. 21nb ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji jest Komendant Główny Policji, który rozpatruje wnioski osób dotyczące przetwarzania ich danych w Krajowym Systemie Informacyjnym Policji.

Celem przetwarzania danych osobowych w KSIP jest realizacja zadań ustawowych, wskazanych przede wszystkim w art. 1 ust. 2 ustawy o Policji. Zgodnie z tym przepisem do podstawowych zadań Policji należą m.in.:

1) ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra;
2) ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji

[211] Szerzej: W. Kotowski, *Ustawa o Policji. Komentarz, wyd. IV,* Wolters Kluwer Business, 2021
[212] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2023 r. poz. 171, z 2022 r. poz. 2600, z 2023 r. poz. 185, 240, 289, 347, 535, 641, 1088)
[213] Zarządzenie nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji (Dz. Urz. KGP 2019 poz. 114)

publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania;

3) inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi;
4) wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców.

Częściowo przyjmuje się, że system ten pokrywa się z systemem KCIK, albowiem wykorzystuje analogiczne technologie komputerowe. Niemniej jednak o systemie KCIK również będzie mowa na kanwie przedmiotowego rozdziału. W centralnej bazie KSIP gromadzone są informacje o sprawcach przestępstw i sposobach ich działania, o osobach poszukiwanych i zaginionych, o osobach, które na mocy decyzji administracyjnych otrzymały zakazy, w tym zakaz prowadzenia pojazdów lub były uprzednio notowane, o kierowcach, którzy otrzymali punkty karne za wykroczenia popełnione w ruchu drogowych, o osobach o nieustalonej tożsamości, o niezidentyfikowanych zwłokach, o osobach posiadających zezwolenie na posiadanie broni, jak również o broni utraconej, o zdarzeniach kryminalnych oraz mających z nimi związek przedmiotami, np. pojazdami, dokumentami itp. Podstawową zawartością tej teleinformatycznej bazy danych jest zawartość tekstowa, niemniej jednak wskazać należy, iż z uwagi na specyfikę tego zbioru, widnieją tam również elementy graficzne w postaci m.in. fotografie sprawców przestępstw, a nadto osób poszukiwanych[214], osób i zwłok o dotychczas nieustalonej tożsamości, portretów pamięciowych i inne[215]. Przedstawione obszary przedmiotowe nieustannie rozwijanej bazy danej KSIP jednoznacznie pokazuje, iż jest to zbiór niezwykle szeroki, zawierający informacje i dane w najszerszym z możliwych zakresów, dotycząca zarówno kwestii dotyczącej osób, zdarzeń, rzeczy spraw jak również obiektów, w tym informacji o lokalizacji zdarzeń, nieruchomości, instytucji przy wykorzystaniu obecnie budowanych map cyfrowych, o których również będzie mowa w kolejnych rozdziałach. Podkreślenia wymaga również fakt, iż dla sprawności i faktycznej funkcjonalności tego systemu, oczywiście nie może on działać w pojedynkę i wymaga spójności i wewnętrznego powiązania z innymi obowiązującymi bazami teleinformatycznymi. I tak np. w ramach KSIP wykorzystywany jest np. System Poszukiwawczy Policji (SPP), który jest narzędziem informatycznym działającym podobnie do wyszukiwarki internetowej, co

[214] Szerzej: I. Sołtyszewski, D. Solodov, *Procedury policyjne poszukiwań osób zaginionych* [w:] E. Gruza (red.), I. Sołtyszewski (red.), *Poszukiwania osób zaginionych,* Wolters Kluwer, 2021, s. 259 i nast.
[215] M. Goc, E. Gruza, J. Moszczyński, *Kryminalistyka czyli o współczesnych metodach dowodzenia przestępstw,* Wolters Kluwer, 2020, s. 24 i nast.

z pewnością wielu kojarzy się z seriali kryminalnych. System ten umożliwia bezpośredni dostęp do wielu baz danych, w tym do wyżej opisanego KSIP, ale również Schengen Information System, Visa Information System, Centrum Ewidencji Ludności PESEL, Centrum Ewidencji Pojazdów i Kierowców CEPIK, jak również Straży Granicznej, więziennictwa oraz bazy REGON. Powiązania te wskazują, iż system ten w znacznym stopniu wykorzystuje nowe technologie oraz metody komunikacji elektronicznej. Obecnie jest on bardzo rozwinięty, niemniej jednak wraz z rozwojem nowych technologii, sukcesywnie dokonywane są w ramach jego funkcjonalności udoskonalenia.

Ogromne zasoby tej bazy danych pozwalają na początkowym etapie postępowania przygotowawczego dokonanie wstępnych weryfikacji, zawężenie kręgu osób podejrzewanych, a niekiedy już na tym etapie możliwie jest bezpośrednie wytypowanie sprawcy przestępstwa. Nadto szeroki zakres informacji przetwarzanych i gromadzonych na kanwie tych baz danych pozwala na zaryzykowanie stwierdzeniem, iż jest to podstawowe narzędzie dla działalności związanej z wykrywaniem przestępstw przez organy prowadzące postępowanie przygotowawcze, zwłaszcza funkcjonariuszy Policji. Bez wątpienia ogromnym atutem tego systemu teleinformatycznego w ogromnym stopniu wykorzystującego nowe technologie, jest zdecydowane przyspieszenie, ułatwienie i usprawnienie działalności organów prowadzących postępowanie przygotowawcze, pozwalające na sprawniejsze wytypowanie sprawców przestępstw, a w konsekwencji pociągnięcie ich do odpowiedzialności karnej. Oczywiście nie ma wątpliwości co do tego, iż ogromny zbiór danych wymaga konsekwentnego wprowadzania i regularnego uzupełniania danych, niemniej jednak zabieg ten ocenić należy jako znikomo uciążliwy w porównaniu do korzyści jakie przynosi funkcjonowanie omawianego systemu informatycznego.

Zasygnalizować nadto jedynie należy, iż w ramach regularnego udoskonalania systemu KSIP, jest on sukcesywnie integrowany z innymi, dotychczas rozproszonymi systemami policyjnymi, które są również niezbędnym elementem działalności organów ściągania. KSIP stanowi bazę danych osobowych dla systemu automatycznej identyfikacji daktyloskopijnej (AFIS)[216] oraz genetycznej bazy danych (GENOM). Warto jedynie wspomnieć, iż na skutek nowelizacji, zgodnie z powszechnie obowiązującymi przepisami, każda osoba skazana

[216] Szerzej: W. Kotowski, *Ustawa o Policji. Komentarz, wyd. IV,* Wolters Kluwer business, 2021 oraz M. Goc, E. Gruza, J. Moszczyński, *Kryminalistyka czyli o współczesnych metodach dowodzenia przestępstw*, Wolters Kluwer, 2020; Zarządzenie nr 28 Komendanta Głównego Policji z dnia 11 sierpnia 2020 r. w sprawie zbiorów danych daktyloskopijnych (Dz. Urz. KGP 2020 poz. 44)

prawomocnym wyrokiem Sądu ma obowiązek poddania się badaniu daktyloskopijnemu, tj. pobrania materiału porównawczego w postaci odcisków palców, które to dane wraz z przypisanymi danymi osobowymi są później gromadzone i przetwarzane w ramach systemu AFIS a na skutek zintegrowania – również systemu KSIP. Nie ma zatem wątpliwości co do tego, iż w ramach systemu teleinformatycznego KSIP są przechowywane najistotniejsze dane dotyczące przestępców oraz przestępstw, popełnianych nie tylko na terenie naszego kraju, ale również za granicą. W związku z tym istnieje ogromna potrzeba odpowiedniego, właściwego i rzetelnego zabezpieczenia tych informacji, które z uwagi na ich przechowywanie w systemie teleinformatycznym narażone są na ingerencję osób niepożądanych.

Kolejnym instrumentem wykorzystującym nowe technologie, który jest niezwykle istotnym środkiem z punktu widzenia postępowania karnego i działalności związanej z wykrywaniem sprawców przestępstw jest baza danych KCIK, o której była mowa wyżej przy okazji omawiania zintegrowanego charakteru najistotniejszego systemu KSIP. KCIK jest to system informacyjny, którego głównym zadaniem jest gromadzenie, analizowanie i przekazywanie danych przy wykorzystaniu metod komunikacji elektronicznej, mających bezpośredni wpływ na skuteczne wykrywanie i ściganie sprawców przestępstw oraz w zapobieganiu przestępczości[217]. Ta baza danych, podobnie jak podstawowy system KSIP, udostępniona jest z znacznym stopniu dla funkcjonariuszy Policji, ale dostęp do niej ma również m.in. Prokuratura czy Straż Graniczna oraz urzędy skarbowe i organy kontroli skarbowej. W literaturze słusznie podkreśla się, iż uruchomienie tego systemu miało decydujący wpływ z zakresie dostosowania w ten sposób Polski do standardów obowiązujących w Unii Europejskiej, albowiem wówczas polskie systemy informacyjne, stały się nieodłącznym elementem Systemu Informacyjnego (SIS), co jest niezwykle ważnym zabiegiem z punktu widzenia wykrywania i ścigania przestępstw, albowiem zwłaszcza przestępstwa gospodarcze coraz częściej popełniane są nie tylko przez obcokrajowców, ale również przy wykorzystaniu podmiotów zagranicznych albo instrumentów z tym związanych, chociażby posługując się numerami rachunków bankowych zagranicznych banków czy numerami telefonów, dla których również właściwy jest zagraniczny operator.

Wskazać należy, iż gromadzenie informacji i danych w ramach tego systemu, które co bardzo istotne są na bieżąco weryfikowane, uzupełniane i modyfikowane na poszczególnych etapach postępowań przygotowawczych w szerokim rozumieniu tego pojęcia, z pewnością

[217] Ustawa z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych (Dz. U. z 2022 r. poz. 2448)

pozwala na stworzenie kompleksowej analizy zjawiska przestępczości. Dzięki temu możliwe jest sprawniejsze, bardziej precyzyjne i szczegółowe diagnozowanie i prognozowanie zjawiska przestępczości. Zgodnie z treścią ustawy[218] gromadzeniu w Krajowym Centrum Informacji Kryminalnych podlegają informacje kryminalne o przestępstwach, osobach, przeciwko którym prowadzone jest postępowanie karne lub w stosunku do których prowadzone są czynności operacyjno-rozpoznawcze, przedmiotach wykorzystanych do popełnienia przestępstwa, lub utraconych w związku z przestępstwem, przedsiębiorcach, spółkach cywilnych, fundacjach, stowarzyszeniach, co do których zachodzi podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa, zgromadzone w rejestrach prowadzonych na podstawie odrębnych przepisów, numerach rachunków bankowych lub rachunków papierów wartościowych, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa lub że gromadzone są na nich środki pochodzące z przestępstwa i in. Analogicznie jak w przypadku systemu KSIP, całokształt przytoczonych okoliczności jednoznacznie i wyraźnie wskazuje na niezbędny charakter tych baz danych, których funkcjonowanie i działalność w sposób oczywisty zmierza do przyspieszenia procesu karnego oraz zdynamizowania wykrywania sprawców przestępstw, pozwalając na wytypowanie pewnych cech już na początku postępowania karnego.

W niniejszym rozdziale omówiono jedynie najistotniejsze z punktu widzenia wykrywania przestępców instrumenty, zwłaszcza bazy danych, które w zakresie swojego funkcjonowania wykorzystują nieustannie prosperujące nowe technologie. Niemniej jednak organy ścigania mają również dostęp do innych, wcale nie mniej ważnych, baz danych, które ułatwiają prowadzenie i nadzorowanie postępowania karnego, umożliwiają w zdecydowanie szybszym i sprawniejszym tempie pozyskanie pewnych informacji. Warto zasygnalizować, iż z powodzeniem funkcjonują również takie bazy danych, których działanie udostępnione jest również dla osób znajdujących się spoza sfery organów ścigania, niemniej jednak wówczas droga zdobycia informacji tam zawartych jest bardziej sformalizowana. Przykładem potwierdzającym założoną tezę jest baza danych zawierająca w swoim zbiorze dane na temat szeroko rozumianej karalności za przestępstwa, przestępstwa skarbowe, także wówczas gdy procedowano na podstawie ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich[219]. W tym stanie rzeczy mowa o Krajowym Rejestrze Karnym[220], w którym oprócz wyżej wspomnianych danych przechowywane i gromadzone za pomocą systemu

[218] Ustawa z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych (Dz. U. z 2022 r. poz. 2448)
[219] Ustawa z dnia 9 czerwca 2022 roku o wspieraniu i resocjalizacji nieletnich (Dz. U. 2022 poz. 1700)
[220] Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2023 r. poz. 1068)

teleinformatycznego są dane dotyczące osób poszukiwanych listem gończym. Oczywiście do wspomnianych informacji przyporządkowane są dane osobowe i teleadresowe danej osoby. Organy ścigania w toku nadzorowanego postępowania przygotowawczego, zwłaszcza w fazie *in personam,* zwracają się o dane dotyczące uprzedniej karalności podejrzanego. Jest to niezwykle istotne z punktu widzenia przyjęcia kwalifikacji prawnej, a nadto zweryfikowania czy w stosunku do danej osoby zachodzi konieczność przyjęcia kwalifikacji dotyczącej popełnienia czynu zabronionego w warunkach recydywy. Poza przywołaną powyżej bazą danych, organy ścigania mają również dostęp do systemu informatycznego CEPIK[221], w którym przechowywane i przetwarzane informacje zarówno dot. ewidencji kierowców jak i ewidencji pojazdów, obejmujące takie dane jak informacje o właścicielach i posiadacz, a także o osobach posiadających wymagane uprawnienia do kierowania pojazdami.

Nadto istotną bazą danych prowadzoną za pomocą nowych technologii, tym razem dotyczącą osób prawnych i innych jednostek organizacyjnych nieposiadających osobowości prawnej, jest system e-KRS, który ma charakter powszechny, co oznacza, że dostęp do danych gromadzonych w jego ramach ma każdy z poziomu telefonu czy komputera lub innego urządzenia posiadającego dostęp do Internetu. Za pośrednictwem strony ministerstwa, tj. strony rządowej, można przy posiadaniu minimalnej wiedzy nt. prowadzonej działalności gospodarczej (nazwa, NIP, REGON, numer KRS) uzyskać pełne informacje na temat danej spółki prawa handlowego czy też fundacji lub stowarzyszenia. W ramach tego systemu udostępniane są dane w postaci siedziby działalności gospodarczej, firmy, osób reprezentujących oraz sposobu reprezentacji, a także przedmiotu działalności gospodarczej, jak również wzmianki dotyczące złożenia obowiązkowego sprawozdania finansowego za dany rok obrotowy oraz dotyczące zawieszenia działalności gospodarczej i inne.

Reasumując poczynione wyżej ustalenia, które oczywiście dotyczyły wyłącznie zagadnień teoretycznych odnoszących się do wykorzystywanych przez organy ścigania baz danych prowadzonych przy wykorzystaniu nowych technologii i systemów teleinformatycznych, jednoznacznie wskazać należy, iż ich funkcjonowanie pełni kluczową i bardzo istotną rolę w procesie wykrywania przestępstw i ścigania ich sprawców. Instrumenty te pozwalają w sposób zdecydowany usprawnić i przyspieszyć generalnie ujmując postępowanie karne, ale również bezpośrednio wpłynąć na szybkość pozyskiwania i przetwarzania gromadzonych za ich pomocą danych, co w następstwie pozwala na

[221] Centralna Ewidencja Pojazdów i Kierowców

sprawniejsze gromadzenie materiału dowodowego, a w konsekwencji ustalenie okoliczności lezących po stronie sprawcy i podjęcie decyzji co do sposobu zakończenia postępowania karnego. Nie ma wątpliwości co do tego, iż brak takich środków bezpośrednio wywołałby skutek dla czasu trwania postępowania przygotowawczego, a nadto nie byłoby wówczas możliwe pozyskanie pełnych danych dotyczących profilu sprawcy i innych okoliczności niezbędnych do zgromadzenia materiału dowodowego pozwalającego na zakończenie postępowania karnego.

Niemniej jednak zasygnalizować jedynie należy, iż w dalszej części pracy powyższe zagadnienia zostaną w pełni omówione również z praktycznego punktu widzenia, tj. ich rzeczywistego wykorzystania w praktyce przez organy ścigania poprzez m.in. omówienie konkretnych sytuacji, w których określone bazy danych są niezbędne i w jaki sposób przyczyniają się do rzetelnego i prawidłowego prowadzenia i nadzorowania postępowania przygotowawczego, niezależnie od fazy, w której się znajduje.

4.2. Pozostałe instrumenty funkcjonujące w oparciu o nowe technologie

Powyżej wskazano najistotniejsze bazy danych wykorzystujące nowe technologie, prowadzone w systemie teleinformatycznym, które w dużym stopniu wykorzystywane są przez organy ścigania w szerokim znaczeniu tego pojęcia. Niezależnie od powyższego, w działalności i funkcjonowaniu organów ścigania istnieje jeszcze całe spektrum instrumentów wykorzystujących nowe technologie. O ile omówienie zagadnień ogólnych związanych z bazami danych prowadzonymi w systemie teleinformatycznym było możliwe w zasadzie w oderwaniu od zagadnień praktycznych, o tyle zagadnienia dotyczące innych środków bez podania konkretnych przykładów są nie tyle co niemożliwe, ale w gruncie rzeczy bezcelowe, albowiem nie pozwoli to na przedstawienie pełnych możliwości tych metod. Mając na względzie powyższe wskazać jedynie należy, iż organy ścigania dysponują różnego rodzaju programami komputerowymi pozwalającymi na analizę uprzednio zgromadzonych danych, w tym np. danych telekomunikacyjnych i danych bankowych. Aspekt ten jest niezwykle istotny w przypadku cyberprzestępstw, albowiem wówczas zdobywa się najwięcej danych o takim charakterze od administratorów domen internetowych czy operatorów sieci komórkowych, ale również od banków.

Jednym z najbardziej powszechnych programów jest System Wsparcia Prokuratora. Jest to program wykorzystujący narzędzia teleinformatyczne, w tym umożliwia również prowadzenie komunikacji elektronicznej na odległość. Oprócz analizy danych, program

posiada wiele narzędzi ułatwiających w znacznym stopniu prowadzenie i nadzorowanie postępowania karnego. Wśród tych narzędzi wyróżnia się m.in. szablony pism procesowych, zwłaszcza postanowień o wszczęciu śledztwa czy postanowienia o przedstawieniu zarzutów. W wymiarze praktycznym jest to narzędzie niezwykle istotne zwłaszcza w przypadku postępowań, w których mamy do czynienia z kilkudziesięcioma czynami lub dużą liczbą osób podejrzanych w sprawie. Program pozwala m.in. na wybranie z listy właściwej kwalifikacji prawnej (uwzględniając również zbieg przestępstw, czyn ciągły czy działanie sprawcy w warunkach recydywy, również wielokrotnej), a następnie generuje osobie prowadzącej postępowanie karne formularz postanowienia, wymagające uzupełnienia jedynie czasu i miejsca popełnienia czynu zabronionego. W zakresie bardziej zaawansowanych narzędzi, które pozwalają na poczynienie ustaleń, które byłyby niemożliwe do zweryfikowania bez tego programu to metody służące do analizy zwłaszcza danych telekomunikacyjnych.

Przez dane telekomunikacyjne w zakresie praktycznej pracy organów ścigania rozumieć należy informacje uzyskane od operatorów sieci komórkowych, dotyczące bezpośrednio danych osobowych i teleadresowych abonenta lub użytkownika numeru telefonów, wykazu połączeń przychodzących i wychodzących (tzw. billingów rozmów) ale także wykazu logowań do stacji BTS. Nadto dane telekomunikacyjne dotyczą również adresów IP i numerów portów źródłowych oraz docelowych, za pomocą których można ustalić w pierwszej kolejności operatora sieci, a następnie tożsamość jego użytkownika. System Wsparcia Prokuratora w zakresie właśnie tych danych umożliwia dokonanie bardzo precyzyjnych ustaleń, pozwalając w ten sposób zminimalizować czynnik czasu i nakład pracy, albowiem wszelkie analizy danych dokonywane są za pomocą systemu teleinformatycznego oraz nowych technologii. Rzeczone analizy realizowane bez tego systemu zajęłyby prokuratorowi z pewnością wiele czasu i nadto nie przyniosłoby tak efektywnych rezultatów jakie udostępnia omawiane oprogramowanie. W odniesieniu do zakresu analiz dokonywanych przez System Wsparcia Prokuratora pozwala on na dokładne ustalenie powiązań pomiędzy ustalonymi numerami telefonów, w tym wskazania ilości, czasokresu i częstotliwości nawiązywanych połączeń, ale – co bardzo istotne – pozwala na stworzenie „mapy" opartej o lokalizację do masztów BTS danego numeru MSISDN. Analiza ta pozwala m.in. na wytypowanie drogi, którą poruszał się użytkownik numeru telefonu, co w zestawieniu z innymi poczynionymi w toku postępowania przygotowawczego okolicznościami niejednokrotnie zdaje się być kluczowe dla ustalenia sprawcy przestępstwa. Nadto zasygnalizować należy, iż rezultaty oraz wyniki analiz dokonanych przez środki udostępnione w ramach Systemu Wsparcia Prokuratora przekazywane są organom ścigania w sposób

niezwykle przystępny i bardzo czytelny, albowiem są one dostarczane w postaci tabel i wykresów, które następnie są przydatne dla dalszych ustaleń i ustalania okoliczności faktycznych popełnienia czynu zabronionego objętego zakresem postępowania.

Niezależnie od powyższego, praktyczny wymiar zastosowania tego systemu teleinformatycznego oraz jego faktyczne możliwości na konkretnych przykładach wraz z pełnym zobrazowaniem możliwych do uzyskania rezultatów zostanie omówiony w kolejnych rozdziałach przy okazji formułowania argumentów przemawiających za postawioną na wstępie niniejszej części pracy tezą, zgodnie z którą System Wsparcia Prokuratora jest naczelnym instrumentem usprawniającym działanie organów ścigania.

Wykorzystującym podobny schemat działania instrumentem udostępnionym stosunkowo niedawno organom ścigania, o którym warto w tym momencie wspomnieć jest ogólnokrajowy i szeroko dostępny system o nazwie „Proksys", który niejako zastąpił dotychczas funkcjonujący system o nazwie „SiP". Dla celów rozprawy na tle kolejnych rozdziałów analizie poddane zostaną poszczególne narzędzia dostępne w ramach tego systemu pod kątem ich przydatności oraz potencjalnego wykorzystania przy okazji procesu wykrywczego cyberprzestępstw. Zasygnalizować jedynie należy, iż jest to system pełniący najbardziej ogólnie rzecz ujmując funkcję bazy danych, gromadzący pełne dane dotyczące prowadzonych postępowań w danej jednostce prokuratury, bazujący na działaniu szeroko rozumianych nowych technologii, udostępnionych dla jednostek prokuratury różnego szczebla.

Rozdział III

Polska jako społeczeństwo informacyjne

Jak wyżej wielokrotnie wskazywano, informacja w obecnie otaczającej rzeczywistości stała się jednym z najbardziej pożądanych dóbr i usług. Fakt postępu technologicznego bezpośrednio wpływa na kształt społeczeństwa, w ramach którego dokonywane są liczne przeobrażenia, niejako również dokonując modyfikacji w zakresie samego modelu społeczeństwa. Nie ulega wątpliwości, iż społeczeństwo informacyjne stanowi nowy wymiar rzeczywistości społecznej w XXI wieku, gdzie najistotniejszą rolę stanowi informacja sama w sobie. Możliwość przekazywania i odbierania informacji za pomocą komunikacji na odległość, przy wykorzystaniu innowacyjnych rozwiązań, pozwala na scharakteryzowanie społeczeństwa według coraz to bardziej zaawansowanych standardów. Postęp technologiczny powoduje rozwój społeczeństwa informacyjnego, który z kolei wprost określa model funkcjonowania państwa, który w ten sposób ewoluuje.

1. Społeczeństwo informacyjne

Na tym etapie przedmiotowej rozprawy, zasygnalizować jedynie należy podstawowe cechy społeczeństwa informacyjnego, albowiem szczegółowa analiza w tym zakresie została przeprowadzona na kanwie pierwszego rozdziału o charakterze teoretycznym, w ramach którego wyczerpująco omówiono zakres definicyjny tego pojęcia. Wśród rzeczonych cech wskazuje się m.in. masowe wykorzystanie sieci teleinformatycznej przez społeczeństwo, uznanie informacji jako jednej z najcenniejszych wartości, funkcjonowanie w oparciu o wiedzę nowoczesną[222], przy wykorzystaniu nowych mediów, pozyskiwanie wszelkich informacji i ich przetwarzanie za pośrednictwem wirtualnej rzeczywistości. Podstawowym warunkiem powstania i rozwoju społeczeństwa informacyjnego jest nowoczesna i rozbudowana sieć telekomunikacyjna, zapewniająca możliwość sprawnego przetwarzania i wymiany informacji[223].

W zakresie podstawowych uwarunkowań społeczeństwa informacyjnego wskazuje się przede wszystkim na rozległą strukturę telekomunikacyjną, w tym swobodny i niczym

[222] M. Witkowska, K. Cholawo-Sosnowska, *Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006, s. 13
[223] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Uniwersytet w Białymstoku, Białystok 2017, s. 42 i nast.

nieograniczony dostęp do wielu operatorów sieci telekomunikacyjnej, wysoki stopień korzystania z informacji, a także wysoki odsetek osób zatrudnionych w szeroko rozumianych usługach[224]. Przyjmuje się, iż pierwsze wzmianki dotyczące społeczeństwa informacyjnego na świecie pojawiły się w latach 60. XX wieku, przy czym źródła upatruje się przede wszystkim w rozwoju Stanów Zjednoczonych, ale również rozpoczęciu komunikacji satelitarnej oraz sukcesywnie rosnącego znaczenia pracowników tzw. umysłowych, których liczba w 1956 roku w Stanach Zjednoczonych po raz pierwszy przewyższyła liczbę pracowników tzw. fizycznych[225].

Skoro jednym z czynników pozwalających na ujmowanie społeczeństwa w wymiarze realnej informacyjności jest stopień rozwinięcia sieci telekomunikacyjnej, analizie poddać należy tą kwestię z punktu widzenia polskiego społeczeństwa. Pojęcie sieć telekomunikacyjna zdefiniowane zostało w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, gdzie wskazano, iż są to „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju".

Jak wynika z raportu o stanie rynku telekomunikacyjnego w Polsce w 2021 roku sporządzonym przez Urząd Komunikacji Elektronicznej[226], w 2021 roku wartość rynku telekomunikacyjnego w Polsce wyniosła 40,8 mld. Z przytoczonych wyników wynika nadto, iż z usług internetu stacjonarnego w tym okresie korzystało niespełna 60% gospodarstw domowych i 8,7 mln użytkowników, zaś Polska była jednym z trzech krajów Unii Europejskiej, w którym ceny usług dostępu do internetu stacjonarnego były najniższe. Użytkownicy internetu mobilnego, świadczonego za pomocą dedykowanych urządzeń typu modemy, karty czy klucze, stanowili w tym okresie 51% użytkowników internetu ogółem, przy czym aktualnie odnotowywany jest spadek ruchu w sieci 4G na korzyść dostępu 5G, z którego w 2026 roku korzystać będzie 81% społeczeństwa polskiego. Analiza wyników otrzymanych na przestrzeni 2020 i 2021 roku wprost dowodzi, iż nieustannie odnotowywany jest wzrost na niemalże wszystkich płaszczyznach w zakresie szeroko rozumianej sieci telekomunikacyjnej, zwłaszcza w zakresie korzystania z usług internetu, wzrostu popularności interesu mobilnego – zwłaszcza jako dostępu 5G. Rok 2021 okazał się przełomowy nie tylko z punktu widzenia wykorzystania

[224] M. Nowina-Konopka, *Istota i rozwój społeczeństwa informacyjnego* [w:] M. Witkowska (red.), K. Cholawo-Sosnowska (red.), *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, Warszawa 2006, s. 20 i nast.
[225] Ibidem, s. 13 i nast.
[226] https://uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2021-r-,431.html (dostęp: 10.05.2023 r.)

dostępu do internetu, ale również pod względem liczby użytkowników telefonii ruchomej, albowiem łączna liczba kart SIM wyniosła 56,6 mln, co daje ewidentnie dostrzegalny wzrost w stosunku do roku poprzedniego. Dane te bezpośrednio wskazują, na nieustannie rosnące dane liczbowe w tym zakresie, na co wskazuje również fakt wzrostu przytoczonych liczb w stosunku do 2020 roku[227] i lat poprzednich. Mając na względzie dane liczbowe wynikające z przytoczonego raportu jak również biorąc pod uwagę fakt rozbudowania nowoczesnej struktury telekomunikacyjnej w Polsce, istnienie na rynku wielu podmiotów będących operatorami sieci telekomunikacyjnej (na koniec 2021 roku 124 przedsiębiorców telekomunikacyjnych) oraz możliwość swobodnego, dowolnego i niczym nieograniczonego wyboru określonego operatora implikuje konieczność stwierdzenia, iż w Polsce panują właściwe warunki do powstania i rozwoju społeczeństwa informacyjnego z perspektywy sieci telekomunikacyjnej jako takiej.

Jak wyżej wskazano, nieustanny postęp technologiczny bezpośrednio implikuje nie tylko możliwość, ale również konieczność opisywania polskiego społeczeństwa przez pryzmat nowych standardów, co z kolei prowadzi do wyodrębnienia podgrup pojęciowych w zakresie definicji społeczeństwa informacyjnego. Nie budzi wątpliwości fakt, iż informacja jest podstawową wartością. Jednoznacznie wskazać również należy, iż główną płaszczyzną, na której dokonywany jest zaawansowany obieg informacji, jej odbieranie, przekazywanie i przetwarzanie odbywa się za pośrednictwem sieci teleinformatycznej, czyli Internetu. Na tej płaszczyźnie, uznać można, iż ukształtowało się pojęcie społeczeństwa masowego. Według słownika PWN jest to termin używany jako określenie społeczeństwa biernych odbiorców, dla którego są charakterystyczne: amorficzność, rozkład więzi międzyludzkich, zanik wartości wyższych, brak zakorzenienia w tradycji, materializm, konformizm, upodobnianie się jednostek do siebie i zanik indywidualności, podatność na manipulację przy użyciu propagandy i reklamy, uniformizacja kultury i jej równanie w dół. Rozumiany analogicznie jak kultura masowa. Na kanwie przedmiotowych rozważań, dla potrzeb pracy, przyjąć jednak należy, iż społeczeństwo masowe to rodzaj społeczeństwa informacyjnego, w którym wymiana informacji odbywa się w zdecydowanej większości przy wykorzystaniu Internetu, zaś samo społeczeństwo cechuje się materializmem, ograniczeniem więzi i kontaktów międzyludzkich, podatnością na wpływy i chęcią dążenia do doskonałości. Przytoczone definicje bezapelacyjnie

[227]https://www.uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2020-r-,391.html(dostęp 10.05.2023 r.)

przejawiają szereg podobieństw, skupiając uwagę na tych samych cechach, niemniej jednak druga definicja zdaje się być bardziej jasna i spójna w odniesieniu do czynionych rozważań.

Jak wyżej podkreślono, fakt rozwoju technologicznego niejako dostarcza możliwości opisywania społeczeństwa według kolejnych cech i standardów, przypisując mu przymiot coraz bardziej zaawansowanego. Nowe technologie bez wątpienia determinują wiele okoliczności i spraw, a ich coraz szersze wykorzystywanie w kolejnych sektorach i branżach, przyspiesza te procesy. Rozprzestrzenienie się pandemii koronawirusa w Polsce i na świecie, w ostatnim dziesięcioleciu stało się najbardziej decydującym czynnikiem implikującym rozwój społeczeństwa informacyjnego oraz wykształcenie się w jego ramach pewnych podgrup o bardziej szczegółowym zasięgu. Konieczność wprowadzenia szeregu regulacji prawnych, na mocy których ograniczono dostęp do wielu instytucji, jak również ograniczono możliwość realizowania pewnych czynności, pośrednio zmusiła społeczeństwo do przeniesienia wielu kwestii do Internetu.

Czas pandemii koronawirusa, to jest lata 2020-2022 odnotowywane są jako znaczący wzrost zainteresowania Internetem, ale również istotne zwiększenie zatrudnienia w ramach pracy zdalnej. Niezależnie od powyższego, wprowadzono szereg rozwiązań umożliwiających załatwienie spraw i problemów za pośrednictwem sieci teleinformatycznej, zwłaszcza w zakresie usług użyteczności publicznej. W tym okresie spopularyzowano portal Internetowego Konta Pacjenta, przy wykorzystaniu którego aktualnie wystawiane są wszelkie recepty, zwolnienia lekarskie, ale również odnotowywane są incydenty udzielonej pomocy medycznej, pobyty w szpitalu czy też zdalna możliwość wyrobienia karty EKUZ. Przytoczone okoliczności wprost wskazują, iż aktualnie w zakresie szeroko rozumianych spraw lekarskich w wymiarze osobistym może zostać załatwiona przez Internet, a tym samym na ten moment możliwie maksymalnie odstąpiono od rozwiązań papierowych. Analogiczny wzrost popularności w tym okresie odnotowano również w przypadku narzędzia jakim jest profil zaufany, który oczywiście z powodzeniem funkcjonował już wcześniej, aczkolwiek potrzeba zrealizowania pewnych spraw, w tym urzędowych, po uprzedniej weryfikacji przy wykorzystaniu właśnie tego instrumentu, niejako wymusiła wzrost zainteresowania w tym zakresie. Na skutek ograniczeń wprowadzonych w związku z pandemią, wiele instytucji państwowych udostępniło możliwość załatwienia spraw za pośrednictwem platform internetowych (np. platforma e-pit), ułatwiając w ten sposób społeczeństwu dostęp do usług użyteczności publicznej. Nadto w związku ze znacznym ograniczeniem możliwości organizowania m.in. spotkań służbowych w wymiarze realnym, przedsiębiorstwa niejako

zmuszone były do poszukiwania innowacyjnych rozwiązań, umożliwiających realizację zadań dotychczas prowadzoną w formie tradycyjnych spotkań. Na skutek tego, w 2022 roku 36,8% przedsiębiorstw organizowało spotkania zawodowe za pośrednictwem Internetu[228].

Pojęcie korzystania z usług e-administracji dotyczy przede wszystkim korzystania ze stron internetowych dotyczących szeroko rozumianej sfery obywatelskiej, w tym m.in. składania deklaracji podatkowych, załatwienia spraw administracyjnych, załatwienia formalności dotyczących zasiłków społecznych, ale także publicznych usług edukacyjnych i zdrowotnych. Z raportu sporządzonego przez Główny Urząd Statystyczny wynika, iż w 2022 roku zakupów przez Internet dokonywało 64,6% Polaków, zaś z usług administracji publicznej przez Internet korzystało 55,4 % społeczeństwa (dla przykładu: w 2021 roku – 47,5%), a największy odsetek użycia Internetu w celu korzystania z usług e-administracji odnotowano wśród osób z wykształceniem wyższym, a najniższy wśród osób z wykształceniem podstawowym. Jak wynika z raportu GUS na koniec 2022 roku ponad 9 mln osób korzystało z aplikacji mObywatel, w ramach której korzystano z elektronicznego prawa jazdy, dowodu rejestracyjnego (mPojazd) praz Karty Dużej Rodziny[229]. W zakresie celów korzystania z Internetu w sprawach prywatnych, jak wynika z raportu sporządzonego przez GUS w 2022 roku, największy odsetek (74,3% ogółu osób) dotyczył wyszukiwania informacji o towarach i usługach, zaś kolejne miejsce zajmowało korzystanie z poczty elektronicznej (69,3%) oraz korzystanie z komunikatorów społecznościowych (64,75)[230]. Wynik w tym zakresie, w odniesieniu do państw Unii Europejskiej, wskazuje, iż największy udział stanowiły osoby wysyłające i odbierające pocztę elektroniczną.

Reasumując powyżej poczynione ustalenia, wskazać należy, iż społeczeństwo informacyjne to takie, w którym większość aktywnych zawodowo osób zajmuje się przetwarzaniem informacji, a narzędzia informatyczne wykorzystywane są szeroko także w związku z innymi formami aktywności obywateli (komunikacją, konsumpcją, edukacją)[231], a informatyzacja służy zwiększaniu efektywności przetwarzania danych[232]. Skoro przyjmuje

[228] Raport Głównego Urzędu Statystycznego, Społeczeństwo Informacyjne w Polsce w 2022 r., s. 130, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,2,12.html (dostęp: 30.06.2023 r.)
[229] Ibidem, s, 133
[230] Ibidem, s. 119
[231] G. Szpor, *Urzędnicy w społeczeństwie informacyjnym*, [w:] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2007, s. 288
[232] G. Szpor, *Administracyjnoprawne problemy informatyzacji*, [w:] J. Supernata (red.), *Między tradycją a przyszłością w nauce prawa administracyjnego. Księga jubileuszowa dedykowana Profesorowi Janowi Bociowi*, Wrocław 2009, s. 719

się, iż społeczeństwo informacyjne zapewnia obywatelom powszechny dostęp i umiejętność korzystania z technologii informacyjnych w celu podnoszenia i aktualizacji wiedzy, ochrony zdrowia i innych usług mających wpływ na wyższą jakość życia, to poczynione powyżej wzmianki na temat popularyzacji dostępu do usług publicznych za pośrednictwem Internetu, wskazują, iż polskie społeczeństwo zakwalifikować należy jako zaawansowany etap społeczeństwa informacyjnego.

2. Status polskiego społeczeństwa na podstawie przeprowadzonego badania ilościowego

Celem zweryfikowania, a w zasadzie oceny stopnia zaawansowania informacyjności polskiego społeczeństwa, przeprowadzono badania ilościowe, których wyniki pozwoliły na wyprowadzenie satysfakcjonujących wniosków. Wybór metodologii przeprowadzenia badań ilościowych wynikał przede wszystkim z faktu, iż wyłącznie ten rodzaj badań zapewniał osiągnięcie zakładanych celów, albowiem liczbowe ujęcie wartości dostarcza możliwości wciągnięcia rzetelnych wniosków oraz podjęcia realnej próby ustalenia statusu społeczeństwa – poprzez faktyczne przeprowadzenie badań wśród dużej ilości osób, przy zapewnieniu zróżnicowania cech grupy badawczej. Celem przedmiotowych badań było ustalenie czy grupa badawcza może zostać zakwalifikowana jako społeczeństwo informacyjne, w tym masowe, jeśli tak to na jakim etapie zaawansowania aktualnie się znajduje. Badania ukierunkowane były nadto na sposób pozyskania informacji, częstotliwość oraz cel korzystania z mediów i komunikatorów społecznościowych i ich rodzaju a także na temat kwestii cyberbezpieczeństwa oraz ewentualnych cyberprzestępstw popełnianych na rzecz osób badanych i świadomości na temat cyberzagrożeń oraz ich samodzielnego zwalczania, ewentualnie przeciwdziałania.

Rzeczone badanie przeprowadzono w wysoko rozwiniętej, z silną pozycją rynkową firmie produkcyjnej, funkcjonującej w oparciu o zagraniczny kapitał – HanseYachts Sp. z o.o. (NIP: 9551000455) z siedzibą przy ul. Prostej 28 w Łozienicy, gm. Goleniów, województwo zachodniopomorskie, której przedmiotem działalności jest produkcja jachtów żaglowych, a która rozpoczęła działalność w 2002 roku. Wybór rzeczonej firmy podyktowany był przede wszystkim charakterem grupy badawczej, która cechuje się różnorodnością w zakresie wieku, płci, wykształcenia i statusu społecznego. Urozmaicenie wśród grupy badawczej pozwoliło na osiągnięcie najbardziej rzeczywistych wniosków. Grupę badawczą w tym zakresie stanowiły osoby różnej płci, w wieku głównie produkcyjnym, to jest od 18 do 68 roku życia, o różnym

wykształceniu – od podstawowego do wykształcenia wyższego. Grupę zróżnicowano według rzeczonych podziałów. Łączna liczba osób w tej grupie badawczej to 100 osób.

W celu podjęcia próby oceny rozwoju oraz potencjału w zakresie kształtowania się społeczeństwa informacyjnego w przyszłości, przeprowadzono również badania ilościowe wśród młodzieży, to jest uczniów I Liceum Ogólnokształcącego im. ppor. Emilii Gierczak w Nowogardzie, przy czym w tym przypadku grupę badawczą stanowili uczniowie w wieku od 15-18 lat, czyli osoby znajdujące się w wieku przedprodukcyjnym. Uzupełniające przeprowadzenie badań w tej grupie badawczej miało na celu wykazanie różnic między osobami w wieku produkcyjnym, a osobami znajdującymi się na etapie kształcenia w szkole średniej, a także scharakteryzowanie społeczeństwa jako społeczeństwa informacyjnego, głównie w zależności od wieku grupy badawczej. Taki sposób przeprowadzenia badań poza sklasyfikowaniem różnic, pozwolił na ich scharakteryzowanie oraz ocenę, a także opracowanie wniosków. Rozpatrywanie obu grup badawczych w aspekcie łącznym pozwoliło na opracowanie wniosków o charakterze całościowym, albowiem wówczas dotyczył będzie grupy badawczej w wieku od 15 do 68 lat, przy jednoczesnym uwzględnieniu różnych grup społecznych. Niemniej jednak dla wyodrębnienia pożądanych wyników, w pełni celowe jest również przeprowadzenie badań porównawczych pomiędzy wyżej wskazanymi dwoma grupami badawczymi, przy jednoczesnym wskazaniu wartości liczbowych w odniesieniu do konkretnej grupy, a następnie na tej podstawie sformułowanie wniosków w wymiarze podstawowym, uzupełniającym oraz porównawczym i szczegółowym.

Badania ilościowe polegały na udostępnieniu obu grupom badawczym kwestionariusza ankiety składającej się łącznie z 25 pytań, gdzie 3 z nich dotyczyły wyłącznie kwestii formalnych odnoszących się do wieku, płci i wykształcenia, czyli cech pozwalających na odróżnienie członków grupy badawczej. W przypadku kwestionariusza przeznaczonego dla osób w wieku przedprodukcyjnym, z uwagi na etap nauki, na jakiej znajduje się grupa badawcza, pominięto pytanie dotyczące poziomu wykształcenia. W pozostałym zakresie, dla obu grup badawczych udostępniono takie same kwestionariusze, które z uwagi na charakter zawartych w nich pytań, uznać należy za uniwersalne i zawierające zagadnienia odnoszące się bezpośrednio do kluczowych problemów badawczych. Sposób sformułowania pytań podyktowany był chęcią eksplorowania kwestii dotyczących społeczeństwa masowego, ale także zweryfikowania stopnia świadomości obywatelskiej w zakresie zagrożeń związanych z masowym działaniem za pośrednictwem sieci teleinformatycznej. Badanie miało również na

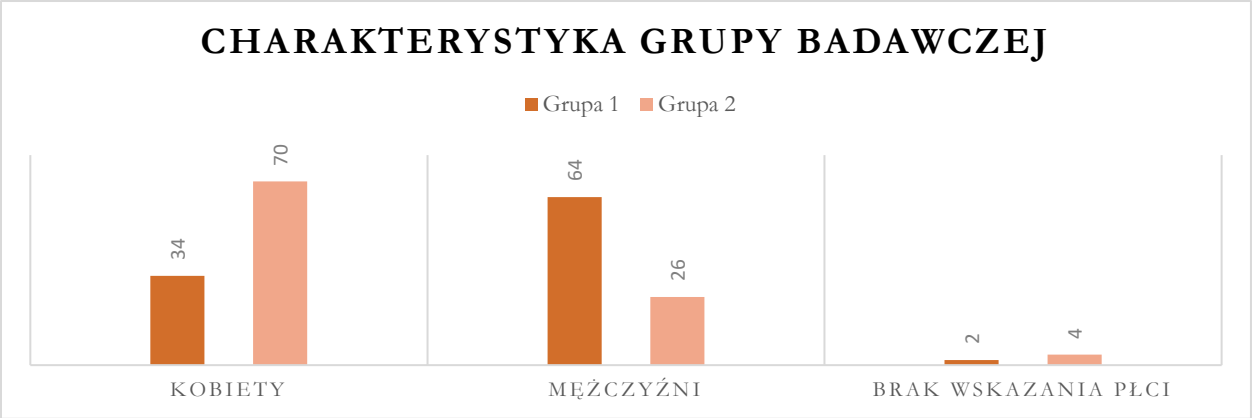
celu ustalenie, na podstawie zamkniętej grupy badawczej, faktycznego korzystania z instrumentów udostępnianych przez organy administracji publicznej w ramach e-usług.

Poniżej przedstawione zostaną wyniki przeprowadzonych badań o charakterze ilościowym, w odniesieniu do konkretnych zmiennych, rozpatrywane z wielu perspektyw, aby wykorzystać maksymalny potencjał przeprowadzonych badań. Rzeczone wyniki przedstawione zostaną nadto w formie wykresów i rysunków, aby zobrazować osiągnięte rezultaty. Na tej podstawie opracowane zostaną wnioski o charakterze podstawowym i szczegółowym w zakresie wszelkich kwestii stanowiących przedmiot badań.

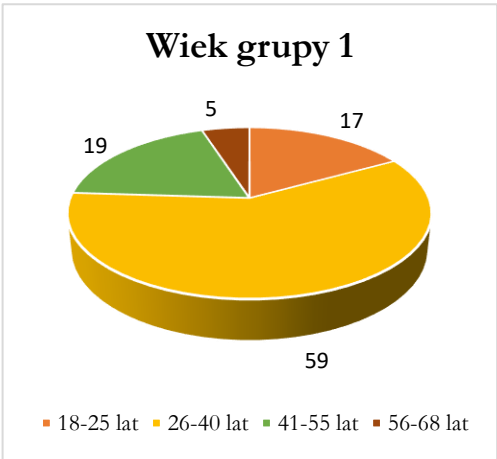
W celu możliwie precyzyjnego i klarownego przedstawienia wyników przeprowadzonych badań, w pierwszej kolejności analizie poddane zostaną rezultaty dotyczące pierwszej grupy badawczej w odniesieniu do konkretnych pytań i na tej podstawie charakterystyka rzeczonej grupy oraz wyciągnięcie wniosków ogólnych i konkretnych. Następnie analogiczna czynność powtórzona zostanie w odniesieniu do drugiej grupy badawczej, a dopiero wówczas przeprowadzona zostanie analiza porównawcza i sformułowane zostaną w tym zakresie kluczowe z perspektywy omawianych zagadnień wnioski. Niezależnie jednak od powyższego, niezbędne jest uprzednie scharakteryzowanie każdej z grup badawczych.

Pierwsza z grup liczyła łącznie 100 członków, przy czym kobiety stanowiły 34%, mężczyźni 64%, a osoby niewyrażające woli wskazania płci – 2%. Wśród rzeczonego kręgu osób badanych, 17% stanowiły osoby w wieku od 18-25 lat, 19% w przedziale 41-55 lat, 5% w wieku 56-68 lat, zaś najliczniejszą grupę stanowiły osoby w wieku 25-40 lat – 59%. W odniesieniu do czynnika zależnego w postaci wykształcenia dominowało wykształcenie średnie (40%) oraz wyższe (34%), pozostały odsetek to osoby z wykształceniem podstawowym (4%) oraz zawodowym (22%). Przytoczone dane wskazują wprost na zadawalające zróżnicowanie grupy badawczej.

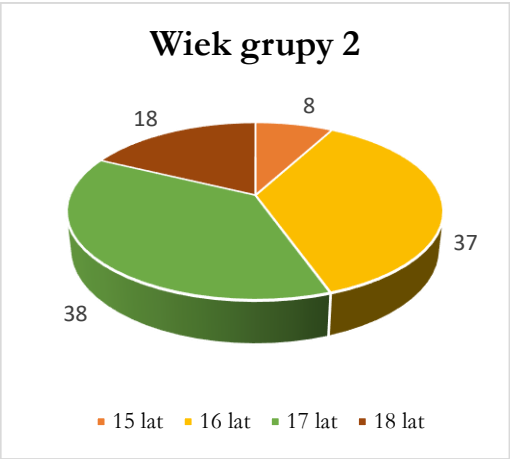
W przypadku drugiej grupy badawczej, liczącej również 100 osób, 70% stanowiły osoby płci żeńskiej, 26 osób zadeklarowało płeć męską, zaś 4% to osoby nie wyrażające chęci wskazania płci, przy czym grupa była zróżnicowana pod względem wieku, albowiem 37% to osoby w wieku 16 lat, 38% w wieku 17 lat, zaś 18% stanowiły osoby z ukończonym 18 rokiem życia, a zaledwie 8% osoby w wieku 15 lat.



Wykres 1



Wykres 2

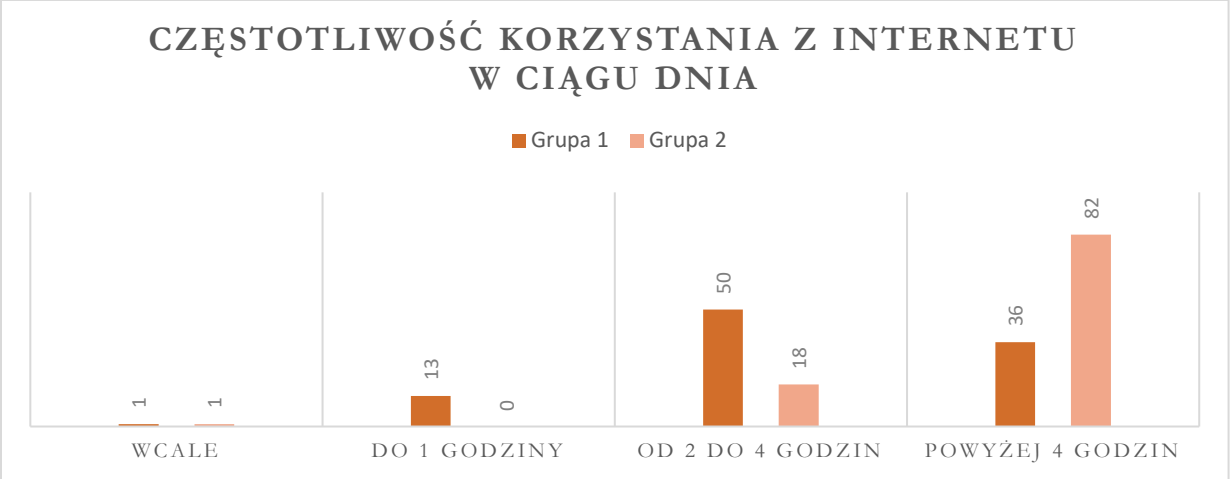


Wykres 3

Jedno z pytań kwestionariusza ankiety udostępnionego dla grupy badawczej w wieku produkcyjnym odnosiło się czasu spędzonego w Internecie w ciągu dnia, przy czym proponowane odpowiedzi brzmiały następująco: a) wcale, b) bardzo rzadko (mniej niż godzinę), c) 2-4 godzin, d) powyżej 4 godzin. Zaledwie 1 osoba, zatem 1% badanych zadeklarowało, iż wcale nie korzysta z Internetu, przy czym był to mężczyzna w przedziale wiekowym 41-55 lat. Aż 86% osób badanych wskazało, iż spędza w Internecie ponad 2 godziny dziennie, przy czym 36% - powyżej 4 godzin. Wśród osób, które zadeklarowały niską częstotliwość korzystania z Internetu w ciągu dnia (13 osób), 77% stanowili mężczyźni.

Analogiczne zagadnienie w drugiej grupie badawczej dostarczyło następujących wyników. Podobnie jak w powyżej przywołanych rezultatach przeprowadzonych badań, zaledwie 1% osób badanych wskazało, iż wcale nie korzysta z Internetu w ciągu dnia, zaś nikt nie zadeklarował korzystania z tej usługi rzadko, to jest mniej niż jedną godzinę dziennie. 18% osób badanych wskazało, iż w Internecie spędza od 2 do 4 godzin dziennie, a pozostali, to jest aż 82% grupy badawczej oświadczyło, iż czas ten wynosi powyżej 4 godzin. Przytoczone

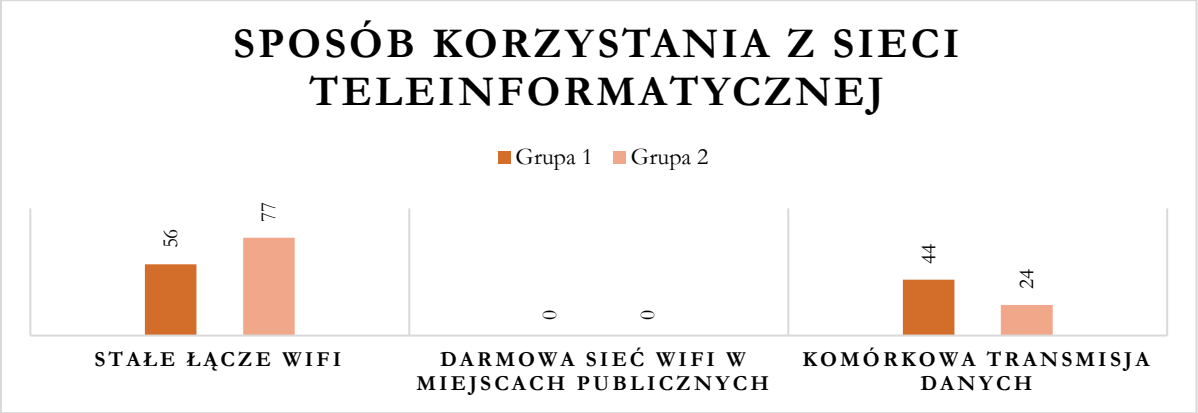
wyniki badań w sposób oczywisty wskazują, iż Internet aktualnie jest środowiskiem stanowiącym duże zainteresowanie wśród osób o różnym wieku i wykształceniu, w żaden sposób nie jest zależne od płci, natomiast w sposób ewidentny z uzyskanych wyników badań wynika, iż osoby poniżej 18 roku życia spędzają znacznie więcej czasu w Internecie aniżeli osoby w wieku produkcyjnym. Fakt oferowania w Internecie w zasadzie nieograniczonego katalogu usług, form spędzenia wolnego czasu, realizacji hobby a także atrakcyjność mediów społecznościowych i komunikatorów sprawia, że zdaje się być to najlepsze miejsce dla klasycznego „złodzieja czasu". Ponad 4 godziny dziennie stanowią co najmniej 17% doby, co przy założeniu, iż 8 godzin poświęcane jest na pracę i taki sam czas na sen, jest to ponad połowa wolnego czasu. Z pewnością nie zawsze czas spędzony w Internecie jest czasem produktywnym, a w wielu przypadkach wynika z negatywnych nawyków, a być może nawet uzależnienia od urządzeń elektronicznych.



Wykres 4

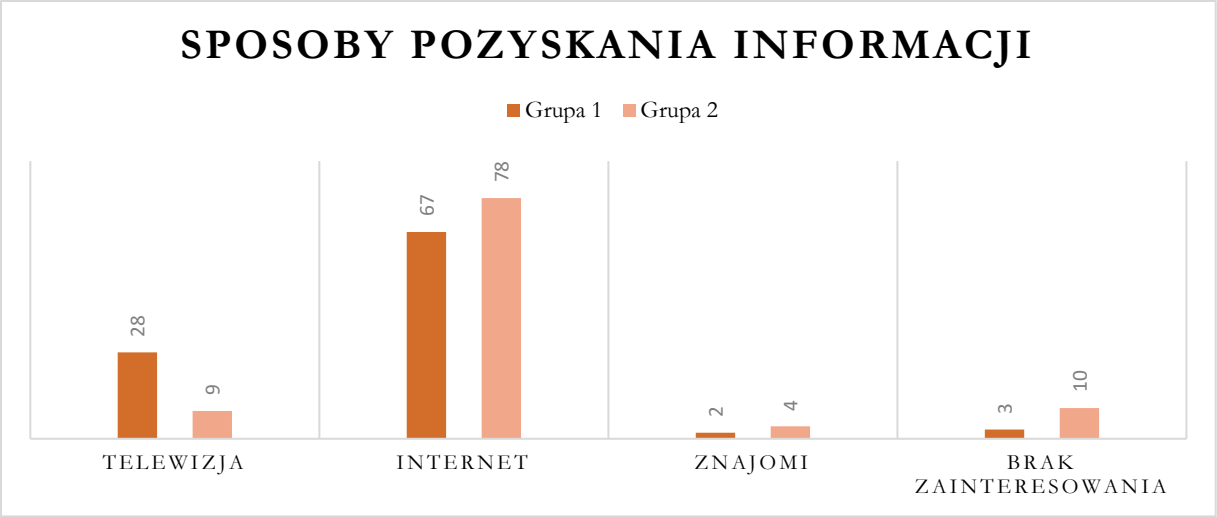
W związku z tym, iż w zakresie zagadnień *stricte* związanych ze społeczeństwem informacyjnym i jego statusem wyróżnia się stopień rozwoju i dostępu do infrastruktury telekomunikacyjnej, kwestia ta również stanowiła przedmiot badań. Aktualnie, jak wyżej wskazano, rynek usługodawców udostępnia szeroki katalog możliwości oraz szeroki wybór zarówno w zakresie łącza, za pomocą którego możliwe jest połączenie z Internetem jak również w zakresie operatora sieci telekomunikacyjnej, za pomocą którego to połączenie nastąpi. W obecnie otaczającej rzeczywistości, dostęp do sieci Wi-Fi stanowi podstawowy standard wielu miejsc, w tym hoteli, ale również restauracji, galerii handlowych, środków lokomocji czy kawiarni. W ramach odpowiedzi udzielonych przez pierwszą grupę badawczą, 56% badanych wskazało, iż korzysta ze stałego łącza/domowej sieci wifi, zaś 44% korzysta z transmisji danych dostępnej w ramach świadczonych usług telekomunikacyjnych bezpośrednio związanych

z abonamentem. W drugiej grupie badawczej 77% osób badanych korzysta z domowej sieci wifi, zaś 24% opowiedziało się, za korzystaniem z telefonicznej transmisji danych. Żadna z badanych osób, z obu grup badawczych nie zadeklarowała korzystania z darmowego łącza udostępnianego w miejscach publicznych.



Wykres 5

W zakresie omawianej kwestii analizie poddać należy odpowiedzi udzielone przez grupę badawczą w ramach kolejnego zagadnienia przedstawionego w kwestionariuszu ankiety, które odnosiło się do sposobu pozyskiwania informacji na temat sytuacji w kraju i na świecie, a zatem wiedzy na temat codzienności, polityki, zdarzeń znaczących zarówno na arenie krajowej jak i międzynarodowej. 95% badanych wskazało, iż w tym celu wykorzystuje środki łączności elektronicznej w postaci telewizji i Internetu, niemniej jednak zdecydowana większość, bo 67% zadeklarowało sieć teleinformatyczną jako przeważający sposób zasięgania podstawowych informacji w życiu codziennym. Zaskakująco niewiele osób, bo wyłącznie 2 osoby wskazały, iż korzystają w tym zakresie z wiedzy i doświadczenia znajomych i współpracowników. Podobne wyniki uzyskano na podstawie badań przeprowadzonych w drugiej grupie badawczej, w której łącznie 87% osób badanych wskazało na Internet i telewizję jako źródło pozyskania informacji, natomiast 10% osób wskazało, iż w ogóle nie interesuje się tym tematem. Uzyskane w tym zakresie wyniki przeprowadzonych badań jednoznacznie potwierdzają postawioną na wstępie tezę, iż informacja stanowi jedną z najbardziej pożądanych usług, a Internet stanowi podstawowy jej nośnik. Niepodważalny jest fakt, iż jako pierwsze wiadomości dotyczące zarówno wydarzeń krajowych, jak i światowych, udostępniane są w Internecie, a dopiero następnie dowiedzieć się można o nich z telewizji. Niemniej jednak nieustanna ewolucja nowych technologii sprawiła, iż to właśnie sieć teleinformatyczna stała się podstawowym źródłem pozyskania informacji, ale nie tylko – na co wskażą kolejno przedstawione wyniki badań.



Wykres 6

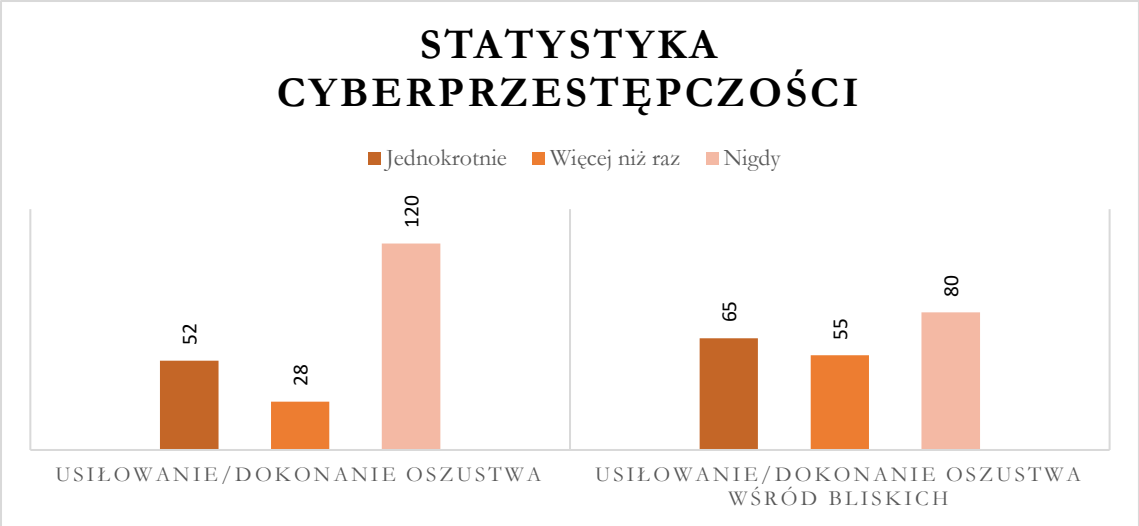
Na kanwie przedmiotowej rozprawy wielokrotnie poruszony zostanie temat negatywnych następstw rozwoju technologicznego rozpatrywanych głównie z perspektywy cyberbezpieczeństwa. Jak na wstępie wskazano, brak jest możliwości dokonania właściwej oceny rozwoju technologicznego i rozpatrywania go wyłącznie jako idealnego środka stanowiącego bezapelacyjną szansę na rozwój na każdej płaszczyźnie. Każda zmiana utożsamiana jest nie tylko z pozytywnymi aspektami, ale również, a może nawet przede wszystkim z ujemnymi następstwami, które mogą wywołać kolejne konsekwencje.

W tym miejscu wyraźnie wskazać należy, iż przestępstwa popełniane za pośrednictwem sieci teleinformatycznej stanowią aktualnie największą liczbę przestępstw popełnianych na terenie kraju. Wśród czynników warunkujących ten fakt wskazać należy przede wszystkim sukcesywnie rosnący wzrost zainteresowania Internetem jako takim, zakupami dokonywanymi w sieci, co z kolei powoduje, iż miejsce to zdaje się być doskonałym środowiskiem dla przestępców. Nadto rozwój technologiczny dostarcza sprawcom przestępstw narzędzi coraz bardziej niezawodnych, zapewniających im anonimowość, powodujących maskowanie ruchu w sieci, dzięki czemu mają oni poczucie nieuchwytności i bezkarności. Niemniej jednak kwestia ta poddana zostanie szczegółowej analizie na kanwie kolejnych rozdziałów. W nawiązaniu do poczynionych rozważań ocenie poddać należy kolejne z zagadnień stanowiące przedmiot badań ilościowych, a odnoszące się bezpośrednio do cyberprzestępczości. Przedstawienie w ramach kwestionariusza ankiety pytań dotyczących tego zagadnienia miało na celu ustalenie – w zamkniętej grupie badawczej – poziomu cyberprzestępczości oraz ewentualnie wysokości utraconego mienia.

Spośród osób badanych w ramach pierwszej grupy badawczej, 36% padło ofiarą przestępstwa popełnionego za pośrednictwem sieci teleinformatycznej lub usiłowano wobec niej takiego dokonać, z czego 12% osób zostało oszukanych więcej niż raz. Oznacza to, iż co 3 osoba stała się ofiarą oszustwa (lub innego przestępstwa popełnionego przez Internet), ewentualnie w stosunku do niej usiłowano dokonać takiego przestępstwa, co daje niezwykle zatrważający wynik, a przypomnieć należy, iż grupę badawczą stanowiło zaledwie 100 osób, zatem przypuszczać można, iż tendencja byłaby rosnąca w przypadku zwiększenia liczby osób badanych. Analogiczne pytanie zadano w odniesieniu do osób bliskich ankietowanych. W tym przypadku aż 65% badanych opowiedziało się, iż osoba z ich otoczenia co najmniej jednokrotnie padła ofiarą przestępstwa popełnionego za pośrednictwem Internetu lub usiłowano wobec niej takiego dokonać. 14% osób badanych, w ramach kolejnego pytania, wskazała, iż na skutek ww. zachowań straciła majątek w Internecie, przy czym największa spośród wskazanych kwot to 20.000 zł, czyli zdecydowanie nieprzeciętnej wysokości kwota. Pozostała część, to jest 86% osób zaprzeczyła utracie jakiegokolwiek majątku, co daje pozytywne rokowania i budzi nadzieje, iż użytkownicy Internetu będą bardziej ostrożni podczas działania w sieci.

Dokładnie takie samo zagadnienie stanowiło przedmiot badań ilościowych przeprowadzonych w drugiej grupie badawczej składającej się z osób poniżej 18 roku życia. Wśród osób badanych 28% wskazało, iż jednokrotnie dokonano lub usiłowano popełnić przestępstwo na ich szkodę za pośrednictwem Internetu, zaś 16% osób wskazało, iż taka sytuacja miała miejsce więcej niż raz. Oznacza to, iż 44% osób spośród tej grupy badawczej co najmniej jednokrotnie spotkała się z przestępczym działaniem w sieci osobiście. W odniesieniu do osób bliskich, łącznie 58% osób badanych zadeklarowało, iż rzeczone sytuacje miały miejsce co najmniej jednokrotnie.

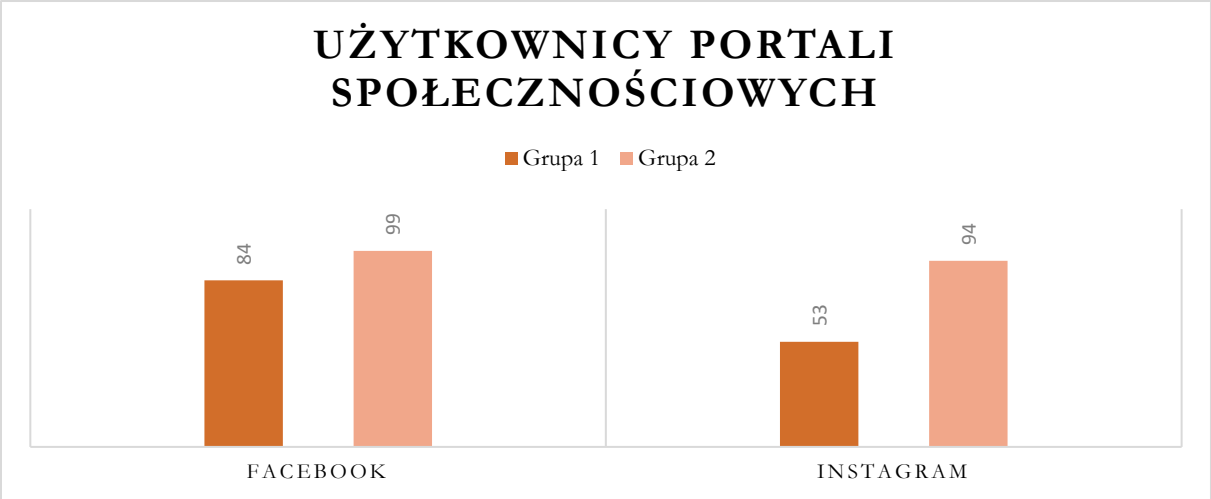
Uzyskane wyniki badań nie pozostawiają wątpliwości co do tego, iż większość osób badanych nie miała bezpośredniej styczności z cyberprzestępstwem, niezależnie od grupy wiekowej. Fakt ten pośrednio wynika z sukcesywnie nagłaśnianych w mediach rożnego rodzaju informacji na temat przestępstw internetowych, sposobów działania sprawców, a także ostrzeżeń przed ochroną swoich danych i majątku. Przekłada się to z kolei nie tyle na zminimalizowanie liczby cyberprzestępstw, ale na bardziej ostrożne poruszanie się w sieci, a w konsekwencji niejednokrotnie uniknięcie utraty pieniędzy lub nieuprawnionego przechwycenia wrażliwych danych.



Wykres 7

Wśród czynników determinujących wzrost liczby cyberprzestępstw popełnianych na terenie kraju, ale jednocześnie warunkujących byt społeczeństwa informacyjnego wskazuje się m.in. dostępność i korzystanie z *social mediów* czyli portali społecznościowych. Aktualnie uznaje się, iż najbardziej popularnymi portalami tego rodzaju jest Facebook, Instagram, Twitter, TikTok. Niemniej jednak z uwagi na chęć konkretyzacji badań, zdecydowano się ograniczyć do dwóch portali spośród ww., które zdają się być dominującymi. Badania przeprowadzone wśród pierwszej grupy badawczej dostarczyły w zasadzie uprzednio możliwych do przewidzenia wyników, albowiem powszechna wiedza wprost wskazuje na potężną liczbę użytkowników rzeczonych witryn. W zakresie portalu społecznościowego Facebook 84% osób badanych wskazało, iż posiada konto na tej platformie, natomiast w odniesieniu do Instagrama – 53%, przy czym zdecydowana większość osób badanych zadeklarowała zarejestrowanie konta na obu serwisach. Badania wskazały nadto, iż wśród osób negujących posiadanie konta na portalu Facebook, zaledwie 3 osoby, to jest 6% spośród 53%, pomimo tego posiadają konto na platformie Instagram, natomiast w odwrotnym kierunku zdecydowanie więcej osób posiada konto na pierwszym, aniżeli drugim portalu.

W przypadku drugiej grupy badawczej 99% osób badanych zadeklarowało posiadanie zarejestrowanego konta na portalu społecznościowym Facebook oraz 94% na portalu Instagram. Wyniki te są w zasadzie bezlitosne i wskazują na bardzo wysokie zainteresowanie portalami społecznościowymi, a w przypadku osób poniżej 18 roku życia wskazują na nieprawdopodobną skalę korzystania z tego rodzaju mediów. Potwierdza się w ten sposób postawiona na wstępie teza w zakresie maksymalnego wykorzystania portali społecznościowych, które z kolei stały się środowiskiem dla sprawców cyberprzestępstw.

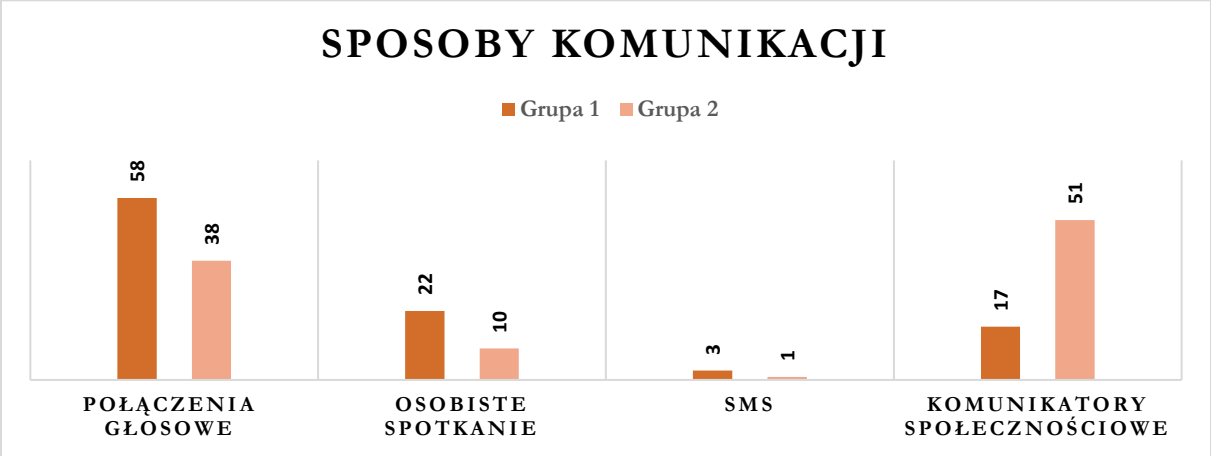


Wykres 8

W tym samym zakresie istotne znaczenie przypisywane jest również komunikatorom społecznościowym, które w obecnie otaczającej rzeczywistości stały się bardzo popularnym środkiem komunikacji elektronicznej. Przyjmuje się, iż ten sposób komunikacji na odległość z powodzeniem zastąpił wiadomości tekstowe przesyłane za pośrednictwem SMS, przy czym komunikatory społecznościowe oferują znacznie szerszy zakres środków komunikacji na odległość, umożliwiając również komunikowanie się za pomocą przekazywania obrazu i dźwięku, nagrań dźwiękowych, wysyłania obszerniejszych plików, zdjęć i nagrań wideo, a nadto poza dostępem do sieci Wifi lub transmisji danych, nie wymaga poniesienia dodatkowych kosztów, w tym opłat abonenckich. Samo pobranie aplikacji również jest bezpłatne i wymaga wyłącznie zarejestrowania użytkownika. Aktualnie wśród najbardziej popularnych komunikatorów, w odniesieniu do których administrator nie wymaga dodatkowych opłat, wskazuje się Messenger administrowany przez Facebook oraz WhatsApp. Mniejszą popularnością wykazuje się Discord i Telegram. Przeprowadzone badania w tym zakresie w grupie badawczej w wieku produkcyjnym wskazują, iż obecnie zaledwie 3% osób komunikuje się za pomocą wiadomości tekstowych SMS, a 22% deklaruje kontakt poprzez osobiste spotkanie. Pozostałą część stanowią połączenia głosowe, które dominują w tej grupie badawczej (58%) oraz komunikacja za pomocą komunikatorów społecznościowych (17%). Niewielki odsetek ostatniej z grup w pewnym zakresie wynikać może z wieku grupy badawczej, albowiem ta odpowiedź najrzadziej wybierana była przez osoby powyżej 40 roku życia.

Wyniki uzyskane na podstawie badań przeprowadzonych w tym zakresie w drugiej grupie badawczej wskazują, iż tylko 1% osób badanych wybiera wiadomości SMS jako sposób komunikacji, 10% deklaruje kontakt poprzez osobiste spotkanie. Zdecydowanie dominującą

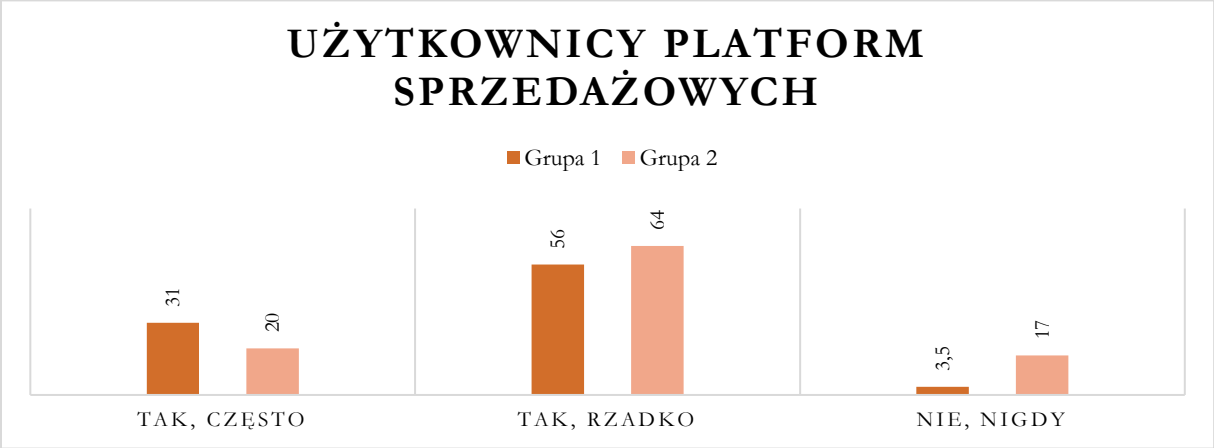
grupę (51%) stanowią osoby wykorzystujące komunikatory społecznościowe, a 38% wybiera połączenia głosowe telefoniczne. Przytoczone wyniki badań potwierdzają powyżej przywołane stanowisko, zgodnie z którym faktycznie wykorzystanie komunikatorów społecznościowych ma ścisły związek z wiekiem użytkowników. Osoby poniżej 18 roku życia zdecydowanie częściej wybierają tą formę komunikacji, aniżeli osoby dorosłe. Niezależnie od powyższego, w obu grupach badawczych, a zatem niezależnie od płci, wieku i wykształcenia, niewielka część społeczeństwa wybiera osobiste spotkanie jako formę komunikacji z innymi ludźmi, co wprost wskazuje na zatracenie cechy bezpośredniości i zdecydowany wybór form komunikacji elektronicznej.



Wykres 9

Niewątpliwie środowiskiem, w którym sprawcy przestępstw popełnianych za pośrednictwem sieci teleinformatycznej uzyskują szersze możliwości osiągnięcia przestępnych celów są różnego rodzaju platformy sprzedażowe. Pierwotnie, kiedy w Polsce dopiero zaczęła pojawiać się cyberprzestępczość, najwięcej tego rodzaju przestępstw popełnianych było przy wykorzystaniu platform sprzedażowych. Z perspektywy czasu uznać należy, iż były to bardzo prowizoryczne i niezbyt wyszukane i skomplikowane metody sprawcze, będące w przeważającej części przypadków tzw. oszustwami zwykłymi. Fakt wzrostu zainteresowania zakupami dokonywanymi za pośrednictwem Internetu niejako dostarcza cybersprawcom możliwości do następczego popełnienia czynu zabronionego. W związku z faktem, iż platformy sprzedażowe w postaci Olx.pl, Otomoto.pl, Vinted.pl a także stosunkowo nowa platforma Marketplace udostępniona przez Facebook są pośrednio instrumentem i środkiem przyczyniającym się do powstania i wzrostu cyberprzestępczości, na kanwie przeprowadzonej ankiety badaniu poddano również stopień korzystania z rzeczonych platform przez grupę badawczą.

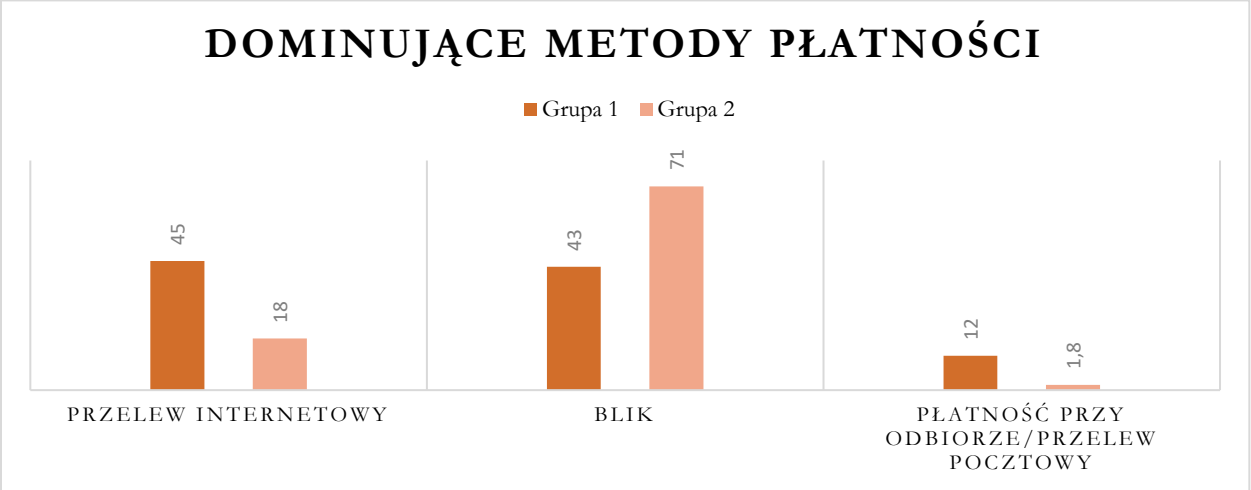
W zakresie pierwszej grupy badawczej 87% osób badanych opowiedziało się za korzystaniem z wyżej wymienionych platform, z czego 31% wskazało, iż wykorzystuje te platformy do dokonywania zakupu/sprzedaży często. Zaledwie 13% osób badanych wskazało, iż nie korzysta z platform sprzedażowych. Zbliżone do wyżej wymienionych wyniki badań uzyskano przy okazji drugiej grupy badawczej, wśród której 84% korzysta z platform sprzedażowych, przy czym 20% czyni to często. Uzyskane w ten sposób wyniki na podstawie przeprowadzonych badań bezapelacyjnie potwierdzają postawioną na wstępie tezę, iż zainteresowanie zakupami realizowanymi za pośrednictwem platform sprzedażowych, aktualnie jest bardzo popularne i wykorzystywane na bardzo dużą skalę, albowiem spośród 200 osób badanych, aż 171 osób to jest niespełna 86% korzysta z rzeczonych usług. Fakt ten bezpośrednio implikuje okoliczność stwierdzenia, iż w sposób oczywisty przekłada się do nie tylko na ilość i częstotliwość cyberprzestępstw popełnianych na terenie kraju, ale również determinuje sposób ich popełnienia oraz określa modus operandi sprawców, który niejako dostosowany jest do potencjalnych ofiar, czyli pokrzywdzonych.



Wykres 10

W związku ze znacznym stopniem wykorzystania platform sprzedażowych, które nierozerwalnie wiążą się również z płatnościami elektronicznymi, w pełni uzasadnione było zweryfikowanie i określenie dominującej metody płatności wybieranej przez użytkowników wyżej wspomnianych platform sprzedażowych, ale też innych usług i płatności realizowanych za pośrednictwem sieci teleinformatycznej. Przedmiotem kolejnego z omawianych zagadnień było przede wszystkim wskazanie głównej metody płatności związanej z szeroko rozumianymi usługami podejmowanymi przez Internet, w tym również sposobu płatności za bieżące rachunki za energię elektryczną, abonament telefoniczny, usługi Internetu itp. Spośród osób badanych, 45% wskazało jako najczęściej wybieraną metodę płatności przelew internetowy, 43% operację

BLIK, a zaledwie 12% osób wskazało, iż wybiera przelew pocztowy tradycyjny lub płatność przy odbiorze. Przytoczone wyniki badań wskazują zatem, iż 88% osób badanych wybiera metody płatności stricte związane z modelem elektronicznym. Nie ma wątpliwości co do tego, iż są najłatwiejsze i najszybsze metody płatności, pozwalające na w zasadzie natychmiastowe osiągnięcie zamierzonego celu, czyli nie tylko zlecenie operacji, ale również odebranie jej przez adresata. W drugiej grupie badawczej wyniki również przedstawiały się w sposób zbliżony do wyżej przytoczonych, albowiem łącznie aż 89% zadeklarowało wykorzystywanie elektronicznych metod płatności, dokonywanych za pośrednictwem sieci teleinformatycznej, z czego aż 71% korzysta z usługi BLIK. Wskazane wyniki badań prowadzą do analogicznych jak wyżej przytoczone wniosków, z tym zastrzeżeniem, iż wśród ludzi do 18 roku życia odnotowany jest zdecydowanie wyższy poziom wykorzystania transakcji BLIK, przy jednoczesnym zmniejszeniu wykorzystania tradycyjnego przelewu internetowego, co bez wątpienia związane jest *stricte* z mobilnym charakterem usługi BLIK oraz możliwością realizacji z poziomu telefonu komórkowego.



Wykres 11

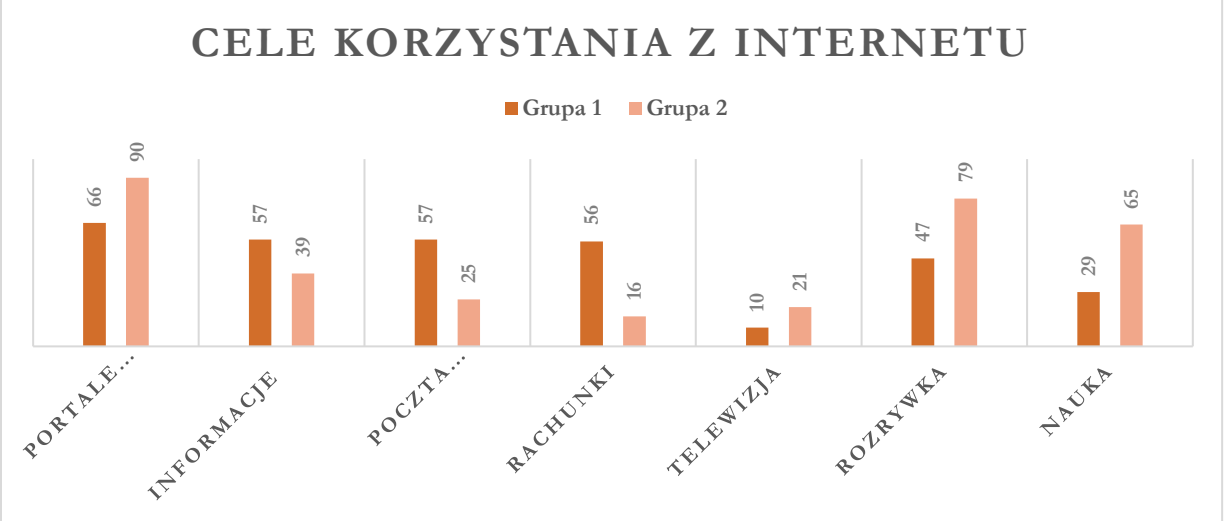
Wskazane powyżej wyniki badań wskazują na potężne zainteresowanie nie tylko portalami społecznościowymi i komunikacją prowadzoną za ich pośrednictwem, ale również zakupami i innymi usługami, które aktualnie udostępniane są za pośrednictwem sieci teleinformatycznej. Przytoczone rezultaty wskazują nadto, iż czas przeznaczony na korzystanie z Internetu w obu grupach badawczych jest w przeważającej części większy aniżeli 4 godziny w ciągu dnia. W związku z tym w pełni celowe i uzasadnione było również zbadanie kwestii celu, w którym użytkownicy Internetu przeznaczają tak znaczną część doby na korzystanie z oferowanych w ten sposób usług. Uzyskane w ten sposób wyniki badań w powiązaniu

z całością badań pozwolą na pełne scharakteryzowanie społeczeństwa i uszczegółowienie dotychczas uzyskanych wyników badań.

W ramach kwestionariusza ankiety udostępniono obu grupom badawczym pytanie wielokrotnego wyboru dotyczące celu korzystania sieci teleinformatycznej. W ramach pierwszej grupy badawczej odpowiedzi zostały w zasadzie rozłożone równomiernie, przy czym najwięcej osób wskazało portale społecznościowe jako główny cel korzystania z sieci teleinformatycznej – 66 odpowiedzi. Pozyskanie informacji ze świata i kraju, korzystanie z poczty elektronicznej oraz opłata bieżących rachunków stanowiło drugą grupę najliczniej udzielonych odpowiedzi, natomiast jak wynika z przeprowadzonej analizy najmniej osób korzysta z Internetu w celach naukowych oraz w celu korzystania z telewizji internetowej.

Uzyskane wyniki na skutek badania przeprowadzonego w drugiej grupie badawczej potwierdziły wyżej przytoczone okoliczności, zgodnie z którymi osoby poniżej 18 roku życia znacznie częściej korzystają z Internetu, ale także cel korzystania z rzeczonej usługi jest inny, co bezpośrednio podyktowane jest potrzebami danej grupy badawczej. Wśród osób badanych, bez wątpienia najwięcej osób (90%) wskazało portale społecznościowe jako dominujący cel korzystania z Internetu, na drugim miejscu wybierając natomiast szeroko rozumianą rozrywkę (79 odpowiedzi), podczas gdy zagadnienie to zostało wskazane przez 47 osób w ramach poprzedniej grupy badawczej. Najmniej odpowiedzi udzielono w zakresie opłaty bieżących rachunków, co bezpośrednio wynika z wieku grupy badawczej. Niemniej jednak zdecydowanie niższe zainteresowanie w odniesieniu do osób dorosłych, odnotowano również w przypadku korzystania z poczty elektronicznej (zaledwie 25 odpowiedzi). Przytoczone wyniki badań wprost wskazują, iż w zdecydowanej większości przypadków czas spędzony w Internecie stanowi ewidentnie tzw. „złodzieja czasu", albowiem rozpatrując uzyskane wyniki badania w perspektywie całości grupy, najwięcej osób korzysta z portali społecznościowych. Wśród osób dorosłych, odnotowuje się również, choć w mniejszym stopniu aniżeli w odniesieniu do rzeczonych portali, zainteresowanie innymi zagadnieniami, takimi jak informacje z kraju i ze świata, załatwienie bieżących spraw życia codziennego, czego nie można stwierdzić w przypadku grupy badawczej poniżej 18 roku życia. Kolejną cechą różnicującą grupy stanowiące podmiot badań, jest nauka jako okoliczność uzasadniająca korzystanie z Internetu, albowiem wśród młodzieży aż 65 osób wskazało tą odpowiedź jako jeden z celów korzystania z sieci, podczas gdy wśród osób dorosłych odpowiedź tą wybrało zaledwie 29 osób. Reasumując czynione w tym zakresie rozważania, wskazać jedynie należy, iż bez wątpienia cel korzystania z Internetu podyktowany jest wiekiem i potrzebami społeczeństwa, aczkolwiek nie pozostawia

wątpliwości, iż portale społecznościowe stanowią główny cel korzystania z Internetu, co stanowi kolejną przesłankę uzasadniającą przyjęcie społeczeństwa sieci, o którym będzie mowa poniżej.



Wykres 12

Z uwagi na fakt bezpośredniego wpływu rozwoju technologicznego na cyberbezpieczeństwo, kwestia ta stała się przedmiotem badań w szerokim zakresie, co ma na celu przeanalizowanie wszystkich możliwych płaszczyzn tej sfery. Rozwój technologiczny niejako dostarcza sprawcom cyberprzestępstw narzędzi umożliwiających popełnianie przestępstw za pośrednictwem Internetu. Niemniej jednak wskazać można wiele okoliczności, które się do tego przyczyniają, a niektóre z nich omówiono powyżej przy okazji przedstawienia wyników przeprowadzonych badań ilościowych w odniesieniu do konkretnych zagadnień kwestionariusza ankiety. Nie ma wątpliwości co do tego, iż czujność użytkowników Internetu w jakiejś części ogranicza możliwości sprawce cyberprzestępców. Sukcesywnie podnoszone w mediach ostrzeżenia dotyczące sposobów popełniania przestępstw na terenie kraju, prowadzenie listy ostrzeżeń przez CERT Polska mają na celu przede wszystkim wzbudzenie wśród użytkowników sieci teleinformatycznej poczucia zagrożenia podczas korzystania z usług tego rodzaju a przede wszystkim bycia czujnym i ostrożnym. Tylko odpowiednia ochrona danych osobowych, a także bycie odpornym na próby wyłudzeń pozwoli na zminimalizowanie liczby cyberprzestępstw popełnianych na terenie kraju. W związku z powyższym przedmiotem badań uczyniono również kwestię świadomości zagrożeń wynikających z działania w Internecie oraz oceny metodologii postępowania użytkowników w przypadku podjęcia wobec nich próby wyłudzenia danych czy też oszustwa popełnionego za pośrednictwem sieci teleinformatycznej.

Pierwsza grupa badawcza, to jest osoby powyżej 18 roku życia na pytanie dotyczące świadomości zagrożeń wynikających z Internetu, w 91% wskazała, iż odpowiednio chroni swoje dane, będąc świadomym takich zagrożeń. Żadna z osób badanych nie zaznaczyła odpowiedzi zawierającej tezę, iż Internet to bezpieczne miejsce. 9% osób badanych wskazała, iż nie zastanawia się nad kwestią cyberbezpieczeństwa, przy czym spośród tej części osób badanych 89% to mężczyźni o wykształceniu zawodowym i średnim, z przeważającą liczbą tych pierwszych, co może wskazywać na to, iż kobiety stanowią grupę bardziej ostrożną podczas działania w sieci. Podobne wyniki uzyskano na podstawie badań przeprowadzonych wśród drugiej grupy badawczej, z tym że 4% osób wskazało, iż Internet to bezpieczne miejsce, co bezpośrednio może wynikać z wieku tychże osób, które w kwestii cyberbezpieczeństwa mogą nie mieć doświadczenia, a tym samym świadomości, będąc obojętnym na potencjalną możliwość popełnienia na ich szkodę przestępstwa. Niezależnie od powyższego, 88% osób badanych w tej grupie wiekowej wskazało na odpowiednią ochronę swoich danych, a tylko 8% wykazało obojętność w tym zakresie. Przytoczone wyniki badań wprost wskazują na wysoki stopień świadomości wśród społeczeństwa w zakresie zagrożeń wynikających z Internetu oraz w zakresie konieczności ochrony swoich danych, czyli podjęcia działań mających na celu pośrednio zapewnienie swojego bezpieczeństwa w sieci. W obu grupach badawczych osiągnięte wyniki wskazują na tożsame wnioski, w związku z czym jako pozbawione sensu jest różnicowanie i wyodrębnianie odmienności w tym zakresie.

Wykres 13

W związku z korzystaniem w bardzo szerokim zakresie zarówno z komunikatorów społecznościowych, portali społecznościowych, różnego rodzaju platform sprzedażowych, na których należy uprzednio zarejestrować konto użytkownika, ale również z usług użyteczności publicznej, co potwierdziły wyżej przedstawione wyniki badań, poruszono również kwestię dotyczącą haseł na różnych platformach. Wiedza ogólna wprost wskazuje, iż administratorzy wielu platform, w celu zapewnienia maksymalnych standardów bezpieczeństwa, podczas rejestracji użytkownika oraz formułowania hasła, wymaga odpowiedniego zróżnicowania pod względem wielkości liter, cyfr i znaków szczególnych, co należy bezapelacyjnie ocenić pozytywnie. Niemniej jednak aktualnie nieustannie zyskuje na popularności metoda dwuskładnikowego uwierzytelniania, która polega na dwuetapowym, wielopoziomowym logowaniu się do danej platformy poprzez sprawdzenie tożsamości użytkownika co najmniej dwukrotnie, to jest np. poprzez podanie hasła, a następnie zaakceptowanie z poziomu innej platformy swojego logowania, czy też wpisanie przesłanego hasła na indywidualnie przypisany numer telefonu czy adres poczty elektronicznej. Głównym celem takiego rozwiązania jest bez wątpienia możliwa maksymalizacja standardów ochrony danych przechowywanych w ramach danej platformy, co ma stanowić pośrednią przeszkodę dla potencjalnych sprawców cyberprzestępstw. W związku z tym, iż rzeczona metoda aktualnie funkcjonuje z powodzeniem, niemniej jednak nadal nie jest obligatoryjna dla użytkowników, w celu weryfikacji poziomu faktycznego zapobiegania przez użytkowników przestępczym działaniom w sieci, poddano tę kwestię analizie w ramach udostępnionego kwestionariusza ankiety. W przypadku pierwszej grupy badawczej, mniej więcej co 2 osoba, albowiem 65% osób wskazało, iż korzysta z tej metody logowania, natomiast zaledwie 4% osób wskazało, iż nigdy wcześniej nie słyszało o metodzie wielopoziomowego, dwuskładnikowego uwierzytelniania. Bardzo zbliżone wyniki uzyskano w przypadku drugiej grupy badawczej, gdzie 67% osób badanych opowiedziało się twierdząco w zakresie tej metody logowania, natomiast 17% badanych wskazało, iż nie ma wiedzy na temat tego sposobu, co jawi się jako zaskakujące zwłaszcza z perspektywy rzeczywistego korzystania z portali i komunikatorów społecznościowych w tej grupie wiekowej oraz zaawansowanej wydawać by się mogło wiedzy na temat narzędzi wykorzystywanych w Internecie. Niezależnie od powyższego pozytywnie należy ocenić środowisko, w którym znaczna większość zna schemat działania logowania wieloetapowego oraz z powodzeniem korzysta z tych rozwiązań, chcąc chronić zasoby swoich danych przechowywanych w wirtualnym świecie.

Wyżej przytoczone zagadnienie nie stanowiło jedynego w zakresie badań, z perspektywy analizy cyberbezpieczeństwa oraz w skrócie ujmując zachowania użytkowników w sieci. W celu stworzenia pełnego obrazu całości grupy badawczej, sformułowano szczegółowe pytania pozwalające na wytypowanie pewnych zachowań użytkowników Internetu w przypadku konkretnej sytuacji bezpośrednio stanowiącej zagrożenie lub takiej, która powinna wzbudzić czujność użytkownika. W drugiej połowie 2022 roku bardzo popularną metodą oszustwa popełnianego za pośrednictwem sieci teleinformatycznej było wysyłanie fałszywych wiadomości tekstowych o nieopłaconych rachunkach za energię elektryczną lub paczkę od popularnego przewoźnika. Dokładny modus operandi sprawcy w przypadku przestępstw tego typu zostanie omówiony na kanwie kolejnego rozdziału, niemniej jednak na potrzeby omawianych zagadnień wskazać jedynie należy, iż metoda ta jest nieprzerwanie wykorzystana przez sprawców, niestety z powodzeniem, albowiem tego typu oszustwo popełniane jest na terenie całego kraju, zaś wyrządzone w ten sposób szkody sięgają nawet kilkuset tysięcy złotych. W związku z aktualnie najbardziej popularnym charakterem tego sposobu działania sprawców, na temat którego prowadzone są bardzo szerokie i głośne ostrzeżenia, badaniu poddano kwestię zachowania się użytkowników w sytuacji potencjalnie niebezpiecznej. Na pytanie dotyczące reakcji na otrzymanie wiadomości tekstowej zawierającej odnośnik do adresu strony internetowej, który ma służyć do uregulowania rzekomej niedopłaty za energię elektryczną lub paczkę, 28% osób badanych z wieku powyżej 18 roku życia, to jest z pierwszej grupy badawczej wskazało, iż weryfikuje autentyczność otrzymanej wiadomości. 6% osób badanych wskazało, iż wchodzi w link, aby uregulować płatność, zaś 76% oświadczyło, iż ignoruje takie wiadomości.

W przypadku drugiej grupy badawczej wyniki przedstawiają się podobnie, zwłaszcza w kwestii ignorowania wiadomości tego typu, albowiem 61% osób badanych wskazało, iż zignorowałoby tego typu wiadomość. Osoby poniżej 18 roku życia są równie ostrożne ,zwłaszcza z perspektywy potencjalnej możliwości utracenia mienia. Nadto, zaledwie 3% osób badanych wskazało, iż wchodzi w otrzymany adres strony internetowej w celu dokonania płatności, bez uprzedniej weryfikacji autentyczności wiadomości. Jest to wynik niższy aniżeli w przypadku grupy badawczej powyżej 18 roku życia. Uzyskane wyniki badań wskazują, iż na skutek podejmowanych działań, ludzie stają się coraz bardziej ostrożni i odporni na techniki socjologiczne i manipulacyjne wykorzystywane przez sprawców cyberprzestępstw, w odniesieniu do konkretnej sytuacji potencjalnie niebezpiecznej. Niezależnie od powyższego, za satysfakcjonujący uznać należy wynik, zgodnie z którym zdecydowana większość osób

deklaruje, iż weryfikuje autentyczność otrzymywanej wiadomości, albowiem oznacza to, iż z sukcesem prowadzona jest akcja nagłaśniania przestępczych zachowań, która spotyka się z właściwą reakcją po stronie odbiorców, czyli potencjalnych pokrzywdzonych – użytkowników Internetu.

Poza powyższymi sytuacjami, które mogą implikować sytuacje co najmniej potencjalnie niebezpieczne, wiele sytuacji skutkujących przestępczym działaniem w sieci teleinformatycznej spowodowanych jest podawaniem przez użytkowników zdecydowanie zbyt wielu danych, w tym danych do logowania do interfejsu bankowości elektronicznej lub pełnych danych dotyczących karty kredytowej. Okoliczność ta bezpośrednio stanowiła kolejny etap przeprowadzonego badania ilościowego, który odnosił się do sytuacji, w której użytkownicy podają kod CVV do karty kredytowej wraz z podaniem jej daty ważności, obok podania jej numeru. Wiele platform wymaga w celach autoryzacyjnych podania rzeczonych danych, przy czym najczęściej dotyczy to rezerwacji biletów lotniczych oraz rezerwacji noclegów na przeznaczonych ku temu stronach internetowych. W przypadku pierwszej grupy badawczej, 40% osób badanych wskazało, iż podaje ww. dane identyfikacyjne karty kredytowej, ale wyłącznie na sprawdzonych stronach internetowych, zaś 57% grupy badanej wskazało, iż nigdy nie podaje takich danych. Zaledwie 3% osób wskazało, iż podaje te dane bez zastanowienia się nad bezpieczeństwem wówczas przeprowadzanej transakcji. Przytoczone wyniki wskazują zatem, iż 97% całości grupy jest ostrożna lub bardzo ostrożna w zakresie podawania tego typu danych, co daje niezwykle zadawalający wynik z perspektywy cyberbezpieczeństwa. Analogiczne badanie przeprowadzono wśród drugiej grupy badawczej osiągając dokładnie takie same jak powyższe wyniki badań, gdzie identyczna liczba osób wskazała takie same jak powyższe odpowiedzi, w związku z tym wnioski w odniesieniu do rzeczonej grupy badawczej przedstawiają się analogiczny sposób jak wyżej.

Wykres 14

Niezależne od wyżej analizowanych sytuacji mogących stwarzać zagrożenie w sieci teleinformatycznej, badaniu poddano również kwestię bezpieczeństwa przechowywania danych związanych z bankowością elektroniczną, ale w świecie rzeczywistym. Często spotykanym zjawiskiem jest przechowywanie danych do logowania do interfejsu bankowości elektronicznej lub kodu PIN do karty płatniczej w pamięci telefonu lub zapisane na kartce w portfelu, co oznacza, że w przypadku potencjalnej kradzieży sprawca uzyskuje w zasadzie automatyczny dostęp do naszych środków gromadzonych na rachunku bankowym, które wówczas narażone są również na ryzyko utraty w wyniku kradzieży. Wśród grupy badawczej składającej się z osób powyżej 18 roku życia, 87 osób zaprzeczyło przechowywaniu tych danych i informacji w sposób opisany powyżej, niemniej jednak 13% grupy wskazało, iż przechowuje dane w tak niebezpieczny sposób. W drugiej natomiast grupie, 73% grupy zaprzeczyło przechowywaniu danych w portfelu w formie zapisku lub w pamięci telefonu,

aczkolwiek 27% twierdząco odpowiedziało na pytanie w tym zakresie. Pomimo wysokiego wskaźnika osób negujących przechowywanie danych w powyższy sposób, część grupy podejmuje ryzyko przechowywania informacji wrażliwych, narażając jednocześnie je na ryzyko utraty i kradzieży. Niestety, uznać należy, niż odsetek osób nie zdających sobie ryzyka z takiego zachowania, jest zbyt duży, zwłaszcza w odniesieniu do możliwości wystąpienia potencjalnie niebezpiecznych sytuacji, niosących negatywne konsekwencje.

Wykres 15

Rozważania w zakresie szeroko rozumianej kwestii cyberbezpieczeństwa, cyberprzestępczości oraz potencjalnie niebezpiecznymi sytuacjami, które pośrednio mogą zostać zainicjowane przez użytkowników Internetu zakończono istotnym z punktu widzenia przedmiotowych rozważań zagadnieniem bezpośrednio odnoszącym się do funkcjonowania organów ścigania. Kwestia wpływu nowych technologii na pracę organów ścigania, stopnia i zakresu tego wpływu zostanie poddania szczegółowej analizie w kanwie następnych rozdziałów, niemniej jednak z uwagi na analizę w ramach przeprowadzonego badania ilościowego kwestii dotyczących bezpieczeństwa w sieci teleinformatycznej, zdecydowano również zbadać kwestię właściwej reakcji na przestępcze zachowania w Internecie. W związku z powyższym w obu grupach badawczych przedstawiono zagadnienie dotyczące sposobu reagowania na przestępstwo popełnione za pośrednictwem sieci internetowej.

W przypadku pierwszej grupy badawczej, to jest osób dorosłych, 93% grupy zadeklarowało niezwłoczne zawiadomienie organów ścigania o popełnionym na ich szkodę przestępstwie, pozostałe 7% wybrałoby inny sposób działania, z czego 3% podjęłoby próbę samodzielnego odzyskania pieniędzy, zaś 4% nie wierzy w wykrycie sprawcy przez organy ścigania oraz wykrycie sprawcy i pociągnięcie go do odpowiedzialności karnej. Nieco odmiennie przedstawiają się wyniki w drugiej grupie badawczej, albowiem 73%

zdecydowałoby się zawiadomić organy ścigania o przestępczym procederze, natomiast 20% osób badanych próbowałoby odzyskać utracone środki we własnym zakresie, a 7% osób nie ma zaufania do organów ścigania w tym zakresie. Pomimo niższego wyniku w przypadku osób niepełnoletnich, z zadowoleniem wskazać należy, iż wyniki przeprowadzonych badań dowodzą, iż panuje powszechne zaufanie do organów ścigania w zakresie ich zdolności i możliwości do wykrycia i pociągnięcia do odpowiedzialności sprawców przestępstw, a w konsekwencji odzyskania utraconych przez pokrzywdzonych środków finansowych, co jest podstawowym zadaniem i celem działania tej grupy zawodowej. Pomimo niskiej wykrywalności sprawców cyberprzestępstw, zaufanie, zwłaszcza wśród osób dorosłych, jest na bardzo wysokim poziomie, a reakcja osób pokrzywdzonych na sytuacje przestępcze w Internecie w zdecydowanej większości przypadków jest jak najbardziej prawidłowa i w zasadzie jedyna w zakresie potencjalnej możliwości odzyskania utraconych pieniędzy, a już na pewno jedyna z perspektywy ewentualnego pociągnięcia do odpowiedzialności sprawcy przestępstwa.

Wykres 16

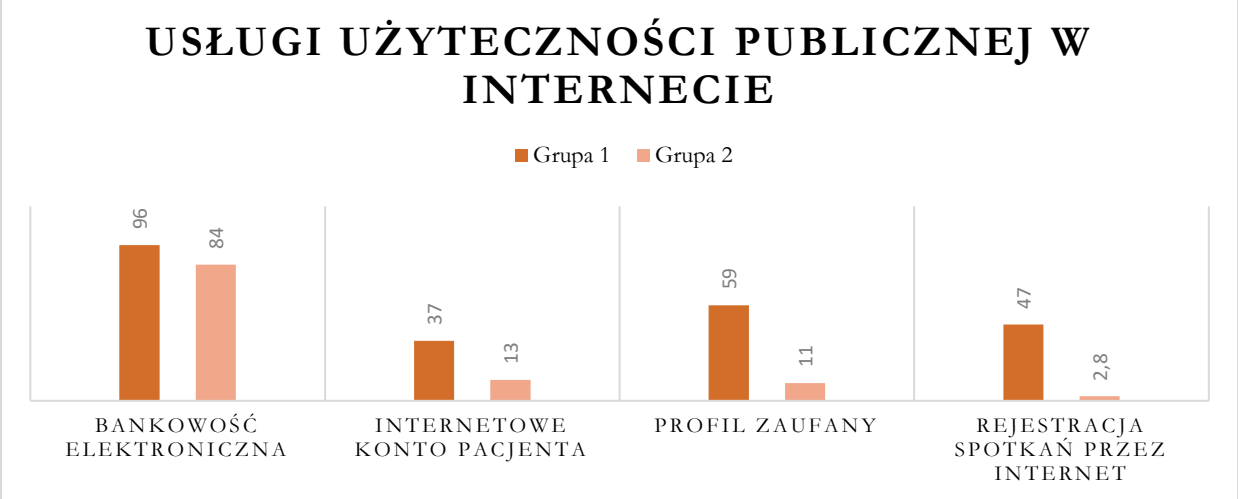
Poza omawianymi kwestiami, czynnikiem pozwalającym na charakteryzowanie społeczeństwa przez pryzmat jego informacyjności, któremu przypisuje się bardzo istotne znaczenie w tym względzie, jest możliwość korzystania z usług użyteczności publicznej za pośrednictwem technologii mobilnych. Aktualnie w Polsce, zdecydowana większość spraw przede wszystkim o charakterze administracyjnym, możliwa jest do zrealizowania za pomocą sieci teleinformatycznej. Społeczeństwu udostępniony został szeroki katalog sposobów przyspieszenia realizacji wielu czynności w kluczowych dziedzinach. Najbardziej popularnymi platformami, których funkcjonowanie przebiega na bardzo wysokim poziomie, posiadającymi zaawansowane struktury i umożliwiającymi realizację szerokiego zakresu czynności w

wymiarze usług użyteczności publicznej jest profil zaufany oraz Internetowe Konto Pacjenta. Obie platformy mają status platform rządowych prowadzonych w domenie gov.pl. Jak wyżej wskazano, na skutek pandemii koronowirusa w Polsce w latach 2020-2022 w sposób znaczny wzrosło zainteresowanie tymi usługami, co wynikało z ograniczenia możliwości bezpośredniego działania w pożądanych sferach. Z uwagi na fakt, iż wiedza w zakresie tych usług ma charakter w zasadzie charakter powszechny, zasygnalizować jedynie należy, iż fakt posiadania konta na profilu zaufanym umożliwia załatwienie spraw, w tym o charakterze urzędowym również na innych platformach oferowanych przez administrację publiczną. Natomiast Internetowe Konto Pacjenta umożliwia dostęp do informacji na temat wystawionych recept, zwolnień, przeprowadzonych zabiegach lekarskich, odbytych wizytach i innych.

W związku z tym, iż fakt skutecznego obowiązywania usług tego rodzaju niejako determinuje społeczeństwo informacyjne, w ramach kolejnych pytań udostępnionych w kwestionariuszu ankiety zapytano obie grupy badawcze o korzystanie z usług tego rodzaju. W katalogu pytań tego rodzaju poruszono również kwestię dostępu i korzystania z bankowości elektronicznej, która w związku z jej szerokim wykorzystaniem może zostać uznana za podobną do wyżej wymienionych usług. Członkowie pierwszej grupy badawczej, w wieku produkcyjnym, w zakresie pytania bezpośrednio odnoszącego się do korzystania z interfejsu bankowości elektronicznej, w 96% zadeklarowali się jako osoby korzystające z tej możliwości, co daje bardzo wysoki wynik, który w zasadzie nie stanowi zaskoczenia, albowiem aktualnie zdecydowania większość operacji finansowych dokonywana jest właśnie w ten sposób. 37% osób ankietowanych wskazało, iż korzysta z Internetowego Konta Pacjenta, a 59% z platformy profilu zaufanego. Zdaje się być to satysfakcjonującą liczbą z uwagi na liczbę osób badanych w ramach tej grupy badawczej. Niemniej jednak wskazać należy, iż ewentualne korzystanie z tych usług bez wątpienia podyktowane jest potrzebą, a jedynie w ramach wyjątku w oderwaniu od konkretnej sytuacji. Oznacza to, że prawdopodobna jest sytuacja, że część osób z grupy badawczej nie znalazła się w sytuacji, w której potrzebowałaby korzystać z tych instrumentów, a gdyby taka sytuacja się zdarzyła – zarejestrowali by swoje konta. Nadto 47% osób badanych wskazało, iż korzysta z możliwości umówienia wizyt u lekarza, w urzędach i instytucjach użyteczności publicznej przez Internet, co również wskazuje, iż mamy do czynienia bez wątpienia ze społeczeństwem informacyjnym w tym wymiarze na niezwykle zaawansowanym poziomie.

W celu przeprowadzenia analizy porównawczej w tym zakresie, co było bezpośrednim celem badań ilościowych, niezbędne jest przedstawienie wyników badań przeprowadzonych

w ramach drugiej grupy badawczej, co dostarczy pełnego obrazu przeprowadzonych badań i pozwoli na sformułowanie satysfakcjonujących wniosków w tym zakresie. Po przytoczeniu wyników badań w tej grupie badawczej, możliwe będzie ich porównanie z wyżej przedstawionymi wynikami badań, w tym również w formie wykresów i ustalenie zależności uzyskanych wyników od czynnika wieku. W zakresie korzystania z usług użyteczności publicznej poprzez technologie mobilne, w przypadku osób poniżej 18 roku życia aż 84% osób korzysta z bankowości elektronicznej. Zaledwie 13% badanych opowiedziało się za dostępem do Internetowego Konta Pacjenta, 11% korzysta z platformy profilu zaufanego, a 24% osób wykorzystuje sieć teleinformatyczną do umówienia wizyt u lekarza czy w innych instytucjach. Porównując rzeczone wyniki z danymi uzyskanymi na podstawie badania ilościowego przeprowadzonego wśród grupy badawczej w wieku produkcyjnym, jednoznacznie wskazać należy, iż zdecydowanie niższy poziom korzystania z tych usług bezpośrednio podyktowany jest wiekiem grupy badawczej. Nie sposób dopatrzeć się innych okoliczności warunkujących te liczby, albowiem fakt niepełnoletności części grupy badawczej niejako pozbawia ich możliwości korzystania z usług o takim charakterze. Niemniej jednak całościowe rozpatrywanie tego zakresu pytań wprost wskazuje, iż 35% wszystkich członków grup badawczych korzysta z platformy profilu zaufanego oraz 25% z Internetowego Konta Pacjenta, zaś 90% korzysta z usług oferowanych przez bankowość elektroniczną.



Wykres 17

Przeprowadzone badanie ilościowe oraz uzyskane na tej podstawie wyniki badań dostarczyły możliwości wywiedzenia wniosków stanowiących odpowiedź na część problemów badawczych będących przedmiotem niniejszej pracy. Co prawda tezy o charakterze szczegółowym zostały wyprowadzone w odniesieniu do każdego z pytań podniesionych w

ramach kwestionariusza ankiety oraz uzyskanych na tej podstawie rezultatów badań, niemniej jednak z uwagi na bardzo złożony, obszerny i kompleksowy ich charakter w celu maksymalnego wykorzystania ich potencjału, warto zwrócić uwagę na wnioski o charakterze generalnym i bardzo ogólnym. O ile nie budzi wątpliwości kwestia przypisania społeczeństwu polskiemu statusu informacyjności, o tyle zastanawiający zdaje się być fakt poziomu jego zaawansowania. Przeprowadzone badanie wśród licznej grupy badawczej, o zróżnicowanych cechach na wielu płaszczyznach, wskazują, iż bezapelacyjnie odnaleźć w niej można zaawansowane cechy struktury społeczeństwa informacyjnego funkcjonującego na bardzo wysokim poziomie. Świadczy przede wszystkim o tym stopień wykorzystania usług użyteczności publicznej za pośrednictwem sieci teleinformatycznej, sposób pozyskiwania informacji oraz komunikowania się ze społeczeństwem, nieprawdopodobnie wysoka popularność portali oraz komunikatorów społecznościowych, a także nowoczesnych metod płatności, a także czas spędzony w Internecie oraz sposób korzystania z niego. Wszelkie czynniki, za pomocą których możliwe jest determinowanie społeczeństwa informacyjnego, odzwierciedlone są w wynikach uzyskanych badań, które bez wątpienia wskazują na istotną wartość informacji jako takiej. Rozwój społeczeństwa informacyjnego podyktowany jest rozwojem technologicznym, który określa to społeczeństwo, nadaje mu charakter i pozwala nadążać nad tym postępem.

3. Społeczeństwo sieci – szanse i zagrożenia

Przytoczone w poprzedniej części pracy wyniki badań implikują konieczność zaprezentowania kolejnego problemu badawczego bezpośrednio odnoszącego się do statusu społeczeństwa sieci. O ile w doktrynie z powodzeniem funkcjonuje pojęcie społeczeństwa sieciowego rozumianego jako jeden z typów społeczeństwa, którego istotą jest sieć relacji społecznych oraz swobodny dostęp do uczestniczenia w różnych organizacjach i grupach społecznych czy kręgach zainteresowań przez jednostkę, o tyle na próżno szukać trafnej i kompleksowej definicji społeczeństwa sieci, które *stricte* związane jest wykorzystaniem nowych technologii przez społeczeństwo. Poczynione ustalenia w powiązaniu z uzyskanymi wynikami badań dają podstawę i bazę do sformułowania rzeczonej definicji na potrzeby przedmiotowych rozważań, a także wyszczególnienia cech społeczeństwa tego rodzaju. Przez społeczeństwo sieci należy rozumieć szczególny rodzaj społeczeństwa informacyjnego, w którym najistotniejszym czynnikiem jest w zasadzie nieograniczony dostęp do sieci teleinformatycznej, a w którym podstawowym sposobem komunikacji jest komunikacja

elektroniczna. Niewątpliwie społeczeństwo sieci i jego byt uwarunkowane jest nieustannym rozwojem technologicznym, które nadaje mu formę, kształt i pewne cechy. Wśród czynników pozwalających zakwalifikować konkretne społeczeństwo do społeczeństwa sieci wskazać należy rozbudowaną strukturę dostępu do Internetu, którego łącze jest satysfakcjonująco szybkie, prowadzenie komunikacji za pośrednictwem sieci teleinformatycznej, pozyskiwanie w taki sam sposób podstawowych informacji, a także dokonywanie zwykłych, bieżących spraw życia codziennego przy wykorzystaniu usług sieciowych.

Przeprowadzone badania ilościowe stanowią jednocześnie odpowiedź na przedmiotowy problem badawczy, albowiem sposób skonstruowania pytań a także udzielone odpowiedzi pozwalają na wyprowadzenie wniosków również na płaszczyźnie ewentualnego przyjęcia bytu społeczeństwa sieci wśród grupy badawczej. Wyniki badań w zasadzie stanowią jednoznaczną odpowiedź na zadane pytanie, albowiem grupa badawcza rozpatrywana w całości spełnia wszystkie wyżej opisane warunki niezbędne dla możliwości przyjęcia społeczeństwa sieci jako społeczeństwa informacyjnego. Świadczy o tym przede wszystkim sposób komunikacji w grupie badawczej, sposób pozyskania informacji na temat otaczającej rzeczywistości, ale również sposób reagowania na sytuacje potencjalnie niebezpieczne w sieci teleinformatycznej, który z kolei wskazuje na pewne doświadczenia oraz zaawansowane struktury tego społeczeństwa.

Niewątpliwie szeroki i w zasadzie nieograniczony dostęp do Internetu w sposób diametralny zmienił wiele mechanizmów, w tym m.in. sposób uprawiania polityki, przekazywania informacji, mechanizmy komunikacji, osiągania poszczególnych etapów wykształcenia czy mechanizmów osiągania sukcesów[233]. Niemożliwe do wyobrażenia zdaje się być aktualnie funkcjonowanie bez dostępu do sieci teleinformatycznej. Nie budzi wątpliwości fakt, iż rozwój technologiczny w tym zakresie w sposób znaczny ułatwił i usprawnił wiele kwestii zwłaszcza z punktu widzenia dostępności do usług, rozrywki, informacji i wiedzy, także osób posiadających pewne ograniczenia czy osób z niepełnosprawnościami, dla których w podstawowej rzeczywistości mogłoby to być utrudnione lub nawet niemożliwe. Niemniej jednak funkcjonowanie w społeczeństwie sieci prowadzi do pewnej alienacji jednostki, pozbawia możliwości pozyskania nowych kontaktów, a tym samym poznania nowych osób i zasięgnięcia innych informacji aniżeli te znajdujące się w kręgu danego użytkownika. Prowadzenie permanentnie komunikacji wyłącznie za pośrednictwem komunikatorów

[233] A. Chęć-Małyszek, *Kultura społeczeństwa sieci a bezpośrednie kontakty społeczne*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy nr 31 (2)/2019

społecznościowych zaburza funkcjonowanie jednostki w grupie, ograniczając wiele aspektów, w tym zasób słownictwa, mowę ciała oraz tzw. kompetencje miękkie, które nabywa się w toku różnych zachowań w grupie, jak również pozbawiając możliwości faktycznego przeżywania pewnych emocji. Nie można zapomnieć również o czasie spędzonym w sieci, który w zdecydowanej większości przypadków nie ma charakteru produktywnego, a wyłącznie stanowi stratę czasu, który pośrednio „kradziony" jest przez Internet, a którego to czasu nie sposób w żaden sposób odzyskać.

Rozdział IV

Praktyczny wymiar komunikacji elektronicznej wśród organów ścigania oraz wymiaru sprawiedliwości

1. Przyczyny wzrostu liczby cyberprzestępstw

Doświadczenie oraz obraz rzeczywistego świata w sposób oczywisty wskazuje, iż rozwój technologiczny na świecie wywiera bezpośredni wpływ na niemalże wszystkie dziedziny życia społecznego, ekonomicznego jak również na obrót prawny. Można również zaryzykować stwierdzeniem, iż rozwój technologiczny niejako „dyktuje" warunki działalności na tych płaszczyznach, na co wielokrotnie wskazywano w poprzednich rozdziałach. Nie ma wątpliwości do tego, iż postęp w tej sferze w zdecydowanej większości pozytywnie wpływa na funkcjonowanie społeczeństwa i ułatwia poprawne i sprawne działanie wielu czynników, niemniej jednak nie bez powodu coraz częściej w doktrynie wskazuje się również na ujemne następstwa postępu technologicznego, zwłaszcza rozwoju komunikacji elektronicznej. Dostęp do coraz nowszych sposobów komunikacji elektronicznej, nowych instrumentów wykorzystujących sieć teleinformatyczną staje się pokusą dla cyberprzestępców, czyli – jak wyżej wskazano – sprawców czynów zabronionych popełnianych z wykorzystaniem sieci teleinformatycznej, w tym środków komunikacji elektronicznej.

Nie sposób nie wspomnieć również o aktualnej sytuacji na świecie, albowiem pandemia wirusa SARS-COV-2 oraz jego pochodnych, która znaczną część działalności przeniosła do trybu zdalnego oraz w wielu sektorach niejako wymusiła pracę za pośrednictwem zwłaszcza Internetu, ale również innych sieci teleinformatycznych, doprowadziła do stworzenia „idealnego" środowiska dla cyberprzestępców. W pierwszej kolejności wskazać należy, iż administracja publiczna w ramach prowadzonej przez siebie działalności znaczną część usług udostępniła w formie internetowej, co oznacza, iż potencjalni petenci mogą składać wnioski i rozwiązywać problemy w formie zdalnej. Taka forma staje się doskonałym środowiskiem dla przestępców, albowiem zachodzi możliwość wykorzystania cudzych danych, podszycia się pod kogoś, a w konsekwencji doprowadzenia do wyłudzenia. Oczywiście wszelkie systemy udostępniane przez takie podmioty są odpowiednio zabezpieczone, zaś dane użytkowników podlegają ochronie, aczkolwiek zastanowić się należy nad tym, czy ochrona i przechowywanie danych wysoko wrażliwych odbywa się w prawidłowy i rzetelny sposób, a co więcej czy prawodawca ma w ogóle możliwość skutecznej ochrony takich danych. Nie ma wątpliwości co

do tego, iż fundamentem ochrony wszelkich danych przechowywanych w bazach systemów teleinformatycznych, jest odpowiednio uprzednio przygotowany również system teleinformatyczny. Rozwój pandemii na świecie wymusił niemalże w trybie natychmiastowym, a co najmniej ekspresowym, przeniesienie wielu dziedzin do sfery Internetu, co bezpośrednio budzi obawę, czy w tak krótkim czasie możliwe jest stworzenie doskonałego zabezpieczenia danych. Oczywiście, wspomniane systemy są sukcesywnie doskonalone, aczkolwiek instrumenty wykorzystywane przez cyberprzestępców, w tym hakerów budzą zdumienie a zwłaszcza wątpliwość, czy wprowadzanie takich danych jest po prostu bezpieczne.

Dane statystyczne wskazujące na charakterystykę przestępstw popełnianych na przestrzeni lat są w zasadzie bezlitosne z punktu widzenia omawianej dziedziny, albowiem wyraźnie i w sposób jednoznaczny wskazują, iż rozwój technologiczny „sprzyja" cyberprzestępcom[234], co w konsekwencji prowadzi do konieczności stwierdzenia, iż w ostatnich latach wzrost cyberprzestępstw był zatrważający. W związku z tym, iż zwłaszcza w zakresie przestępstw popełnianych przeciwko mieniu, tj. oszustw, wyłudzeń, posłużenia się czyimś danymi osobowymi w celu wyrządzenia mu szkody majątkowej, przestępstwa przy wykorzystaniu sieci teleinformatycznej popełniane są najczęściej i na ogromną skalę, często powodując straty sięgające kilku milionów złotych. Cyberprzestępczość, obok ataków terrorystycznych i zmian klimatu jest jednym z największych wyzwań XXI wieku[235]. W 2016 roku stwierdzono 459 internetowych przestępstw związanych z pedofilią (art. 200a § 1-2 k.k.), atakami na zasoby lub urządzenia informatyczne instytucji państwowych lub samorządowych (art. 269 § 1-2 k.k.), atakami na systemy komputerowe lub sieci teleinformatyczne (art. 269a k.k.) oraz udostępnianie urządzeń, programów lub danych służących popełnieniu przestępstw (art. 269b k.k.). Największą liczbę czynów zabronionych (aż 372 przypadki) stwierdzono w odniesieniu do przestępstw związanych z pedofilią. To o 146% więcej niż w roku 2014. Liczba stwierdzonych przestępstw związanych z Internetem lub systemami komputerowymi (np. oszustwa, nękanie, podszywanie się pod inną osobę, pochwała zachowań pedofilskich itd.) w 2016 roku wynosiła 43 957 przypadki, z czego najpopularniejszym czynem było oszustwo (40 778 przypadki). W 2018 roku stwierdzono w Polsce 3,6 tys. przestępstw związanych z phishingiem i e-bankowością. Rosnąca liczba internetowych przestępstw bankowych na

[234] Szerzej: P. Ślęzak, *Prawo mediów*, Wolters Kluwer, Warszawa 2020
[235] W. Filipkowski, *Przestępczość z użyciem komputerów i ich sieci [w:]* E.W. Pływaczewski (red.) *Kryminologia. Stan i perspektywy rozwoju*, Wolters Kluwer, 2019, s. 511 i nast.

świecie spowodowała, że Światowe Forum Ekonomiczne w badaniu „Global Risks Report" uznało cyberprzestępczość za największe ryzyko biznesowe w 2020 r.[236]

Ogromny i wzbudzający niepokój wzrost liczby przestępstw popełnianych przy wykorzystaniu sieci teleinformatycznej, w związku z podstawowym zadaniem organów ścigania, tj. ściganiem sprawców przestępstw, bezpośrednio nakłada na nich obowiązek natychmiastowego reagowania oraz konieczność doboru metod ścigania przestępców i wykrywania przestępstw, które będą przede wszystkim skuteczne, a jednocześnie pośrednio zrealizują również cele prewencji generalnej[237]. Nie bez powodu w różnych jednostkach prokuratur na terenie całego kraju, zwłaszcza w jednostkach wyższego szczebla, tj. prokuraturach okręgowych oraz regionalnych, powoływane są zespoły do spraw cyberprzestępczości, również cyberprzestępczości zorganizowanej, w skład której wchodzą prokuratorzy, będący specjalistami z zakresu cyberbezpieczeństwa, asystenci prokuratorów, jak również informatycy. Niejednokrotnie zespoły takie prowadzą i nadzorują postępowania przygotowawcze zbiorcze z całego kraju, na szkodę wielu osób, dysponując instrumentami umożlwiającymi skuteczne wykrycie sprawcy bądź sprawców. W związku z rozwojem cyberprzestępstw oraz regularnie zwiększającą się popularnością cyberbezpieczeństwa, organy ścigania muszą wypracować pewien algorytm działania, który musi być dopasowywany odpowiednio do danej sprawy w zależności od rodzaju cyberprzestępstwa oraz regularnie udoskonalany z uwagi na sukcesywnie pojawiające się nowe sposoby popełniania przestępstw. Oczywisty zdaje się być fakt, iż nieodzownym elementem takiego algorytmu muszą być pewne systemy teleinformatyczne, w tym bazy danych, ale również narzędzia umożliwiające analizę danych telekomunikacyjnych, danych wykorzystanych w celu popełnienia czynu zabronionego. Zatem odpowiedzią na przestępstwa popełniane przy wykorzystaniu komunikacji elektronicznej są wykorzystujące te same metody instrumenty udostępnione dla organów ścigania. Wyłącznie taki schemat pozwoli na skuteczne wykrywanie cyberprzestępstw oraz ściganie ich sprawców.

Jak poprzednio wielokrotnie wskazano, charakterystyka oraz rodzaj cyberprzestępstw jak również sposób działania sprawców podyktowany jest pośrednio rozwojem nowych technologii oraz udostępnianiem coraz to nowszych sposobów komunikacji elektronicznej.

[236] Międzynarodowy projekt badawczy: *Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości*, zrealizowany przez Instytut Wymiaru Sprawiedliwości https://iws.gov.pl/centrum-analiz-strategicznych/cyberbezpieczenstwo-grupy-wyszehradzkiej-na-rzecz-zapobiegania-przyczynom-przestepczosci/wiecej/ (dostęp 20.05.2023 r.)

[237] Art. 53 § 1 k.k., M. Mozgawa (red.), *Kodeks karny, komentarz aktualizowany*, LEX, 2023

Obecnie katalog rzeczonych przestępstw jest bardzo szeroki[238], sposób działania sprawców pomimo olbrzymiej szkodliwości jest bardzo ciekawym zjawiskiem. W związku z czym analizie poddane zostaną konkretne rodzaje cyberprzestępstw z precyzyjnym opisem działania sprawców, jak również analizą algorytmów działania organów ścigania z jednoczesnym podaniem przykładów spraw oraz powołaniem się na rzeczywisty stopień wykrywania sprawców takich przestępstw w prokuraturach rejonowych, które w zdecydowanej większości zajmują się tego typu postępowaniami przygotowawczymi, nie zapominając jednakże o cyberprzestępstwach popełnianych na ogromną skalę, w tym w ramach zorganizowanych grup przestępczych, które również zostaną poddane szczegółowej analizie. W ramach tego rozdziału omówione zostaną instrumenty wykorzystane przez sprawców, możliwie najdokładniej, tak aby podjąć próbę oceny dotychczas wypracowanych metod wykrywania sprawców przestępstw

Praktyczne aspekty działalności organów ścigania, zwłaszcza w zakresie cyberbezpieczeństwa zostaną poddane szczegółowej analizie. Nie sposób ominąć również organów wymiaru sprawiedliwości, na które nałożone zostały kluczowe obowiązki i zadania w związku z rozwojem nowych technologii. W tym zakresie uwaga zostanie zwrócona na rozwiązania prawne wprowadzone na skutek pandemii wirusa covid w kraju i na świecie, ponieważ prawodawca udostępnił szereg środków wykorzystujących nowe technologie oraz komunikację elektroniczną. W doktrynie wielokrotnie podnoszono wątpliwości w zakresie funkcjonowania w takim stanie rzeczy podstawowych i obowiązujących ogólnych zasad procesu. W związku z tym dogłębnej analizie zostanie poddana również ta kwestia w celu podjęcia próby oceny, czy rzeczywiście wprowadzone rozwiązania zaburzają działanie fundamentalnych zasad.

1.1. Instrumenty wykorzystywane przez sprawców cyberprzestępstw

Analogicznie jak w przypadku wszystkich innych czynów zabronionych, tak również w przypadku cyberprzestępstw dla bytu czynu zabronionego wymagane jest podjęcie pewnego zachowania po stronie sprawcy – w formie działania czy zaniechania, zupełnie bez znaczenia pozostawiając w tym przypadku jego zamiar, który oczywiście z punktu widzenia prawnokarnej oceny czynu bywa decydujący, niemniej jednak obojętny pozostaje na tle niniejszych rozważań. Powszechnie, niejednokrotnie potocznie mawia się, iż każdy sprawca pozostawia po sobie ślad, a powiedzenie, iż „nie ma zbrodni doskonałych" miejmy nadzieję, że będzie można

[238] Szerzej: D. Dajnowiocz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E.W. Pływaczewski (red.), *Badania kryminologiczne a praktyka. Perspektywa krajowa i międzynarodowa, 2021*

ocenić jako trafne również z punktu widzenia sprawców cyberprzestępstw, co jednak zostanie ocenione w dalszej części przedmiotowego rozdziału. Podstawą rozważań w tym zakresie jest jednoznaczne przyjęcie, iż cyberprzestępcy działają za pośrednictwem szeroko rozumianej sieci teleinformatycznej, niejednokrotnie wykorzystując komunikację elektroniczną, a zatem podstawowego punktu zaczepienia w ustaleniu jego tożsamości, należy właśnie szukać w środkach wykorzystujących nowe technologie, albowiem to tam sprawcy zostawiają „ślady" swojego działania, co absolutnie nie oznacza, iż należy zamykać algorytm działania organów ściągania wyłącznie na tej sieci, ponieważ wiele informacji można odczytać również spoza niej. Praktyka wskazuje, iż są trzy podstawowe (co nie oznacza, że jedyne) elementy pozwalające na identyfikację sprawcy, które pojawiają się w większości przestępstw popełnianych za pomocą i przy wykorzystaniu sieci teleinformatycznej.

Pierwszym z nich jest numer MSISDN (ang. Mobile Station International Subscriber Directory Number) – numer abonenta sieci komórkowej (potocznie: numer telefonu). Numer MSISDN jest przechowywany na karcie SIM lub USIM znajdującej się w aparacie, oraz (po stronie sieci) w rejestrze abonentów macierzystych. Każdy numer abonenta przypisany jest do określonego operatora sieci telekomunikacyjnej, z których najpopularniejszymi w Polsce są Orange Polska S.A., T-Mobile Polska S.A., Polkomtel Sp. z o.o. oraz P4 Sp. z o.o. Od 25 lipca 2016 roku na polskim rynku istnieje obowiązek rejestracji wszystkich kart SIM, a wykorzystywane obecnie przez użytkowników karty przedpłacowe (pre-paid) musiały zostać zarejestrowane przed 1 lutego 2017 roku[239]. Oznacza to, iż każda zakupiona karta SIM musi zostać zarejestrowana przez jej użytkownika poprzez podanie danych osobowych w postaci imienia i nazwiska, adresu zamieszkania oraz numeru PESEL. System teleinformatyczny, w którym przechowywane są dane obarczony jest jednakże ogromną wadą, która pośrednio udaremnia jego byt i funkcjonalność, a także cel jego działania, albowiem system ten nie weryfikuje czy podane dane są zgodne z numerem PESEL i czy są faktycznie do niego przypisane, co więcej – nie weryfikuje prawdziwości numeru ewidencyjnego PESEL, a zatem można podać tam numer fałszywy, a system przyjmie każdą wartość, która będzie prawidłowa z punktu widzenia ilości cyfr. Okoliczność ta stała się doskonałym zapleczem dla sprawców przestępstw, albowiem w przypadkach, w których potrzebują wykorzystać numer MSISDS, mogą go zarejestrować na przypadkową osobę zwaną potocznie „słupem" lub też po prostu podać fałszywe dane.

[239] Rozwiązanie wprowadzone na mocy ustawy z dnia z 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2021 r. poz. 2234 ze zm.)

Niezależnie od powyższego, pomimo tego, iż zakładając, że sprawca posłużył się fikcyjnymi danymi podczas rejestracji karty sim lub wykorzystał dane osobowe osoby trzeciej w tym celu, nie zamyka to organom ścigania możliwości do pozyskania dodatkowych informacji posiadając właśnie informację o numerze abonenta. Właściwy dla danego numeru telefonu operator sieci telekomunikacyjnej zobowiązany jest do przechowywania konkretnych danych dotyczących użytkownika numeru telefonu i informacje te nie ograniczają się wyłącznie do jego danych teleadresowych, a dotyczą również tzw. billingów, czyli historii rozmów głosowych i tekstowych prowadzonych przez tego użytkownika a także wykazów logowań to stacji BTS, co z kolei umożliwia wytypowanie lokalizacji, w której sprawca działał. Nadto operatorzy udostępniają dane dotyczące chociażby wszelkich numerów telefonów współpracujących z kartami SIM o określonym numerze. Sposób pozyskania wyżej wymienionych danych oraz możliwości ich dalszego wykorzystania, jak również instrumenty służące do ich analizy dokonywanej przez organy ścigania zostaną precyzyjnie umówione w kolejnym podrozdziale przy okazji omawiania algorytmu działania mającego na celu wykrycie sprawców przestępstw.

Kwestia przypisania numeru telefonu do konkretnego operatora sieci telekomunikacyjnej analogicznie przedstawia się w przypadku kolejnego instrumentu wykorzystywanego przez cyberprzestępców w zasadzie z największą częstotliwością, czyli adresu IP. Adres IP (ang. Internet Protocol Address) to numer identyfikacyjny nadawany komputerom lub innym urządzeniom łączącym się z siecią, który zapewnia im prawidłową komunikację. W systemie dziesiętnym zapisywany jest za pomocą liczb z zakresu 0-255 oddzielonych od siebie kropkami. Jak wyżej wskazano, adres ten przypisany jest do konkretnego operatora sieci telekomunikacyjnej, wśród których najpopularniejsze są w zasadzie te same co dla numerów telefonów, na które przykładowo wyżej wskazano, niemniej jednak w przypadku adresów IP tych operatorów jest znacznie więcej, albowiem dodatkowo pojawia się kwestia tzw. operatorów lokalnych, prowadzących sieci osiedlowe, lokalne, obsługujących m.in. tzw. stałe łącza. Rzeczeni operatorzy przechowują informację na temat użytkowników adresów IP, zwłaszcza w postaci danych osobowych jak również danych teleadresowych, w tym adresu, pod którym zarejestrowana jest usługa oraz charakter obsługiwanego łącza. W przypadku omawiania kwestii adresu IP, którym posługiwał się sprawca cyberprzestępstwa wspomnieć należy o jednym ważnym aspekcie, który niekiedy uniemożliwia identyfikację sprawcy po numerze IP. Dla prawidłowego ustalenia tożsamości użytkownika adresu IP w przypadku zwracania się do operatora sieci telekomunikacyjnej

o dane retencyjne, których pojęcie zostało uprzednio precyzyjnie wyjaśnione, jako konieczne jawi się również wskazanie tzw. numeru portu źródłowego a niekiedy również docelowego. W związku z tym, że konkretny adres IP często wykorzystywany jest przez wielu użytkowników końcowych, dla identyfikacji konkretnego adresu IP niezbędne jest wskazanie konkretnego numeru portu źródłowego, który to numer pozwoli w pełni na ustalenie tożsamości użytkownika tego właśnie adresu. Numer portu źródłowego w literaturze określany jest jako 16-bitowa liczba całkowita zaprojektowana specjalnie do przechowywania protokołu używanego do przechowywania danych. Służy do identyfikacji konkretnych portów sieciowych poprzez posiadanie odpowiedniego adresu IP i protokołu zastosowanego do połączenia. Zdecydowanie rzadziej występującym wymogiem ze strony operatorów sieci telekomunikacyjnych jest wskazanie numeru portu docelowego, aczkolwiek zdarzają się sytuacje, w których prawidłowe ustalenie użytkownika adresu IP niekiedy wymaga wskazania tego numeru. Podobnie jak w przypadku numeru portu źródłowego, numer portu docelowego o długości 16 bitów określa do jakiej aplikacji przeznaczony jest konkretny pakiet danych.

Kolejnym instrumentem wykorzystywanym przy okazji lub w celu popełnienia czynu zabronionego za pośrednictwem szeroko rozumianych nowych technologii, który potocznie można nazwać „śladem" zostawionym przez sprawcę jest adres poczty elektronicznej, zwany najprościej rzecz ujmując adresem mailowym. Powszechnie wiadomo, iż podanie adresu mailowego jest nierzadko wymogiem skutecznego utworzenia i zarejestrowania konta użytkownika na portalach społecznościowych, platformach sprzedażowych a także złożenia wniosku o kredyt czy pożyczkę za pośrednictwem Internetu lub utworzenia w ten sposób rachunku bankowego. Wyżej wspomniane okoliczności wykorzystywane są przez sprawców do popełnienia czynu zabronionego, zatem nie bez powodu wspomina się o nich właśnie w tym miejscu. Podobnie jak w przypadku dwóch wskazanych na wstępie instrumentów, tj. numeru telefonu oraz adresu IP, adresy poczty elektronicznej obsługiwane są przez odpowiednich administratorów domeny poczty elektronicznej, którzy przechowują informacje i dane dotyczące użytkowników, którzy zarejestrowali swoje konta na ich domenach. W Polsce istnieje wielu administratorów takich domen, wśród których wyróżnić można najpopularniejszą Grupę Wirtualna Polska S.A., Axel Ringer Springer S.A., Grupa Onet.pl. Aktualnie bardzo zyskuje na popularności zagraniczna domena gmail.com, która obsługiwana jest przez zagraniczną grupę Google. Pozyskanie przez organy ścigania wiedzy na temat adresu poczty elektronicznej sprawcy otwiera wiele drzwi, albowiem na tej podstawie możliwe jest wytypowanie kolejnych danych retencyjnych, które przeanalizowane w odpowiedniej

kolejności pozwolą na zidentyfikowanie i ustalenie tożsamości sprawcy przestępstwa. Administrator domeny adresu mailowego przechowuje nie tylko dane osobowe i teleadresowe zarejestrowanego użytkownika, ale również podany przez niego numer telefonu, dodatkowy tzw. adres mailowy wspierający a także wykaz logowań do interfejsu poczty elektronicznej jak również adres IP wykorzystany podczas rejestracji. Jak już wskazywano, uzyskane w ten sposób dane, mogą być podstawą do pozyskania kolejnych danych zbliżających organy ścigania do sprawcy popełnionego czynu zabronionego.

Przytoczone instrumenty mają charakter jedynie wyliczenia przykładowego, mieszczą się one w katalogu otwartym, w przypadku którego nie sposób enumeratywnie wymienić wszystkich środków wykorzystywanych przez cyberprzestępców, albowiem w związku z nieustannym rozwojem technologicznym, metody przez nich stosowane są sukcesywnie udoskonalane, ulepszane, modyfikowane – niejednokrotnie w sposób niemożliwy do natychmiastowego ustalenia przez zespoły zajmujące się ich ściganiem. Dopiero w przypadku powtarzającego się schematu działania, organy ścigania są w stanie uchwycić nowy sposób działania sprawców i wówczas przyjąć „tarczę obronną" modyfikując odpowiednio uprzednio przyjęte algorytmy reagowania, mające na celu wykrycie sprawców cyberprzestępstw. W zależności od rodzaju cyberbezpieczeństwa oraz od sposobu działania przestępców, mniej lub bardziej widoczne będą różnice w doborze przez nich instrumentów działania oraz wykorzystania wyżej wskazanych, wykorzystując również bardzo często działanie innych czynników. Dla pełnego zrozumienia, możliwie maksymalnego zobrazowania i przedstawienia tej kwestii z praktycznego punktu widzenia, w pełni celowe i uzasadnione zdaje się być bliższe omówienie tych instrumentów w powiązaniu z konkretnym rodzajem cyberprzestępstwa.

1.2. Rodzaje cyberprzestępstw oraz *modus operandi* działania sprawców

Sposób działania sprawców cyberprzestępstw co do zasady podyktowany jest przede wszystkim rodzajem popełnionego przestępstwa, ale również uwarunkowany jest szeregiem innych czynników w tym zamiarem sprawcy, celem jaki zamierza osiągnąć, wartością rzeczywistej szkody, skalą i rozmiarem jego działania, tj. czy działa na szkodę jednej bądź kilku osób, rozciągnięciem działania w czasie i wieloma innymi, o istnieniu których organy ścigania i potencjalni pokrzywdzeni nawet nie mają pojęcia.

Dokładne i rzetelne omówienie *modus operandi* przestępstw popełnionych przy wykorzystaniu nowych technologii wymaga w pierwszej kolejności omówienia rodzajów i przykładów cyberprzestępstw, a dopiero na ich podstawie wytypowanie i przeanalizowanie

nowych technologii wykorzystanych przez sprawców, a następnie stworzenie „idealnego" algorytmu działania organów ścigania będącego najbardziej trafną i satysfakcjonującą reakcją na zachowanie cyberprzestępców. Rodzaje cyberprzestępstw w *stricte* teoretycznym wymiarze zostały dosyć szczegółowo omówione przy okazji drugiego rozdziału, w którym dokładnie poruszono kwestie definicyjne, zatem z teoretycznego punktu widzenia nie ma potrzeby dalszego pochylania się nad tym zagadnieniem[240]. W związku z tym, że siatka pojęciowo-teoretyczna została już omówiona, istnieje perfekcyjna możliwość do płynnego przejścia do zagadnień w zasadzie całkowicie praktycznych opisujących sposoby działania sprawców cyberprzestępstw z jednoczesnym omówieniem środków komunikacji elektronicznej przez nich wykorzystanych dla celów przestępczych.

1.2.1. Oszustwo metodą „na wnuczka"

Rozważania w tym zakresie zdecydowanie powinny zostać otworzone przez jedno z najbardziej popularnych przestępstw zaliczanych do katalogu omawianej materii, które w zasadzie zakwalifikować można jako najstarsze spośród tych będących przedmiotem omawianych zagadnień, a mianowicie oszustwo metodą „na wnuczka" czy też o analogicznym *modus operandi* „oszustwo metodą „na policjanta". Nie bez kozery właśnie ten sposób działania sprawcy zostaje wskazany w pierwszej kolejności, o czym zdecydowała m.in. rozpowszechniona w kraju i na świecie praktyka działania sprawców, medialny wydźwięk tego rodzaju spraw, sukcesywne pojawianie się coraz to bardziej zorganizowanych grup przestępczych, jak również aksjologiczna odsłona tego przestępstwa, która nie bez powodu wzbudza tak wiele negatywnych emocji, albowiem przestępstwa te popełniane są co do zasady na szkodę osób starszych, nieporadnych ze względu na wiek. Wskazać należy, iż w rozumieniu polskiego kodeksu prawnego za przestępstwo oszustwa uważa się instrumentalne działanie sprawcy ukierunkowane na osiągnięcie korzyści majątkowej polegające na doprowadzeniu do niekorzystnego rozporządzenia mieniem poprzez wprowadzenie pokrzywdzonego w błąd, na skutek czego ponosi on szkodę, zazwyczaj w wymiarze materialnym[241]. Przestępstwo oszustwa stypizowane jest w art. 286 § 1 k.k. i to właśnie ten przepis przyjmowany jest co do zasady jako kwalifikacja prawna dla danego przestępstwa, przedstawiając ją niekiedy – w zależności od konkretnych i indywidualnych okoliczności w związku z art. 65 § 1 k.k. wówczas kiedy sprawca działa w ramach zorganizowanej grupy przestępczej, co zazwyczaj ma miejsce w

[240] Szerzej: W. Filipkowski, *Przestępczość z użyciem komputerów i ich sieci* [w:] E.W. Pływaczewski (red.) *Kryminologia. Stan i perspektywy rozwoju*, Wolters Kluwer, 2019
[241] Art. 286 § 1 k.k., M. Mozgawa (red.), *Kodeks karny, komentarz aktualizowany*, LEX, 2023

przypadku oszustw metodą na wnuczka[242]. Jak wyżej wskazano omawiane przestępstwo popełniane jest zazwyczaj w ramach zorganizowanej grupy przestępczej, w której każdy uczestnik grupy ma odpowiednio przygotowaną rolę. Im więcej osób działa w ramach takiej grupy, tym większe wyzwanie dla organów ściągania, albowiem ustalenie ich tożsamości jest znacznie utrudnione a niekiedy nawet niemożliwe. Po raz pierwszy ten rodzaj przestępstwa odnotowany został na terenie kraju w poprzedniej dekadzie, a zatem z punktu widzenia rozwoju technologicznego całkiem dawno. Pierwotnie sposób działania sprawcy był bardzo niedopracowany, a sprawcy najczęściej byli obcokrajowcami, w związku z czym pojawiający się u nich charakterystyczny akcent był często punktem wyjścia dla organów ścigania.

Oszustwo na wnuczka czy też na policjanta jest odpowiednio wcześniej przygotowaną składową wielu działań i skierowane jest przede wszystkim na szkodę osób starszych, w podeszłym wieku, nieporadnych ze względu na wiek, którzy zazwyczaj nie mają odpowiedniego rozeznania i wielokrotnie dysponują większą gotówką przechowywaną zazwyczaj w ramach domowego zacisza, a nie lokując ją na rachunkach bankowych. Przestępczy proceder, poza oczywiście uprzednim przygotowaniem odpowiedniego zaplecza techniczno-osobowego zorganizowanej grupy przestępczej, rozpoczyna się od wykonania połączenia głosowego do potencjalnej ofiary. Sprawca najczęściej wówczas podaje się za wnuczkę lub wnuczka, którzy znajdują się właśnie w krytycznej sytuacji, która może zostać uratowana poprzez zapłatę odpowiedniej sumy pieniędzy. Zazwyczaj sprawcy wskazują na okoliczność spowodowania przez krewnego wypadku śmiertelnego, a wyłącznie zapłata odpowiednio wysokiej kary grzywny spowoduje uniknięcie odpowiedzialności karnej przez członka rodziny. Aktualnie brak jest jakichkolwiek danych potwierdzających to, iż sprawcy w rzeczywistości znają tożsamość osoby, do której dzwonią jak również mają jakąkolwiek wiedzę na temat członków jej rodziny. Niemniej jednak, rozmowa telefoniczna jest przez nich tak naprowadzona, że niejednokrotnie pokrzywdzony właściwie zmanipulowany w obliczu stresującej sytuacji podaje dane zarówno swoje jak i właściwego członka rodziny. Po sprowokowaniu pokrzywdzonego w ten sposób, iż wskaże on dokładnie jaką gotówką dysponuje, sprawca podaje konkretne wskazówki w jaki sposób ma dojść do jej przekazania. Wówczas najczęściej pojawia się kolejny członek grupy przestępczej, który odbiera od pokrzywdzonego wyłudzoną gotówkę, a następnie – celem zminimalizowania ryzyka oraz zapewnieniu anonimowości kierującego grupą – przekazywana jest jeszcze przez kolejnych

[242] Wyrok Sądu Apelacyjnego w Warszawie z dnia 23 października 2019 roku sygn. II AKa 382/18, LEX nr 2759496

kilka osób zanim trafi do docelowej osoby. Sposób działania sprawcy bądź sprawców wcale nie jest skomplikowany i nie wymaga przede wszystkim ogromnego zaangażowania w zakresie jego przygotowania, niemniej jednak rzeczone przestępstwo ewidentnie zakwalifikować należy jako wysoko społecznie szkodliwe. Podejmując próbę prawnokarnej oceny tego czynu, nie ma wątpliwości co do tego, że zachowanie sprawców wypełnia znamiona przestępstwa oszustwa spenalizowanego w art. 286 § 1 k.k. Ewidentnie działanie sprawców nastawione jest na osiągniecie korzyści majątkowej, ujemne następstwo po stronie pokrzywdzonego również istnieje, albowiem dochodzi do niekorzystnego rozporządzenia mieniem, a sprawca bez wątpienia wprowadza pokrzywdzonego w błąd co do okoliczności rzekomego zdarzenia z udziałem jego krewnego[243].

W związku z tym, iż przedmiotowe przestępstwo omawiane jest niejako w kontekście wykorzystanych w celu jego popełnienia nowych technologii, które są fundamentem rozważań na tle przedmiotowej pracy, przeanalizować należy rodzaj i sposób posłużenia się środkami komunikacji elektronicznej w tym przypadku. Nie bez powodu ten rodzaj przestępstwa został wskazany jako pierwszy, albowiem sfera ta nie jest w przypadku tego *modus operandi* bardzo rozbudowana. Podstawowym elementem łączności sprawcy z potencjalnym pokrzywdzonym jest sieć komórkowa, albowiem co do zasady za pośrednictwem telefonu dochodzi do popełnienia czynu zabronionego[244]. Oczywiście najczęściej sprawca posługuje się tzw. zastrzeżonym numerem telefonu, czyli swoistego rodzaju maskowaniem numeru MSISDN, który najczęściej w aparacie odbiorcy wyświetla się jako „numer zastrzeżony" lub „numer prywatny". Powszechnie przyjmuje się, iż wówczas nie ma możliwości ustalenia rzeczywistego numeru, którym posługiwał się sprawca. Nic bardziej mylnego. Organy ścigania dysponują środkami, które w sposób bezpośredni umożliwiają „odkrycie" numeru, a następnie ustalenie danych teleadresowych jego użytkownika, a nawet określenie lokalizacji, w której wówczas działał. Procesowy sposób pozyskania przywołanych danych telekomunikacyjnych omówiony zostanie w kolejnym podrozdziale dot. narzędzi wykorzystywanych przez organy ścigania w związku ze ściganiem sprawców cyberprzestępstw.

Mając na względzie popularność oraz ugruntowaną praktykę w zakresie przestępczej działalności sprawców przestępstw (oczywiście w negatywnym wydźwięku tego

[243] Wyrok Sądu Apelacyjnego w Warszawie z dnia 20 grudnia 2018 r. sygn. II AKa 420/18, LEX nr 2622689
[244] Szerzej: W. Filipkowski, *Przestępczość z użyciem komputerów i ich sieci* [w:] E.W. Pływaczewski *(red.) Kryminologia. Stan i perspektywy rozwoju*, Wolters Kluwer, 2019

sformułowania) pochylić należy się nad kwestią rzeczywistej wykrywalności sprawców, a precyzyjniej ujmując nad kwestiami statystycznymi w tym zakresie. Ogólnodostępne dane nie wskazują co prawda na dokładne informacje dotyczące skali przestępstw, w których udało się ustalić sprawców w odniesieniu do takich spraw, które zostały zakończone umorzeniem postępowania przygotowawczego na zasadzie art. 322 § 1 k.p.k. wobec niewykrycia sprawcy przestępstwa. Niemniej jednak, przynajmniej w ostatnim pięcioleciu, w zdecydowanej większości postępowań przygotowawczych, których przedmiotem jest oszustwo metodą „na wnuczka" czy też oszustwo o zbliżonym *modus operandi*, organom ścigania „udaje się" przerwać łańcuch zorganizowanej grupy przestępczej, eliminując chociażby jedno, a niejednokrotnie więcej niż jedno, ogniwo[245]. Dogłębna analiza prowadzonych w tym zakresie postępowań wskazuje, że nie zawsze co prawda udaje się pociągnąć do odpowiedzialności karnej tzw. kierującego grupą przestępczą, który uzyskuje największą korzyść majątkową w związku z tym procederem, to jednak przeciwko członkom grupy, których rola polegała m.in. na odbiorze środków pieniężnych od pokrzywdzonego, ich transporcie, dalszym przekazaniu, bardzo często kierowane są akty oskarżenia do właściwych rzeczowo i miejscowo sądów[246]. Oczywiście przytoczony wniosek wcale nie determinuje konieczności stwierdzenia, iż sprawcy rzeczonego przestępstwa w zasadzie pozostają bezkarni, ponieważ zdarzają się również sytuacje, w których dochodzi do skutecznego wykrycia sprawcy, a następnie osądzenia go przed wymiarem sprawiedliwości.

1.2.2. Oszustwo „na pracownika banku". Phishing, malware oraz spoofing.

Przy okazji analizowania i opisu pojęcia cyberprzestępczości w poprzednich rozdziałach wskazywano również na rodzaje cyberprzestępstw, które w związku z częstotliwością ich popełniania, stały się aktualnie jednymi z najbardziej popularnych przestępstw popełnianych w latach 20. XXI wieku[247]. Wówczas wskazywano na charakterystyczny rodzaj cyberprzestępczości tzw. phishing[248], czyli specyficzny rodzaj oszustwa polegający na wyłudzeniu danych, np. numeru karty kredytowej wraz z kodem CVV lub dostępu do bankowości elektronicznej[249]. Sprawca, w celu osiągnięcia korzyści

[245] Wyrok Sądu Apelacyjnego w Białymstoku z dnia 16 listopada 2017 r., sygn. II AKa 178/17, LEX nr 2437805
[246] Postanowienie Sądu Najwyższego z dnia 3 listopada 2021 roku, sygn. III KK 320/21, LEX nr 3275322
[247] I. Stańczuk, Dane osobowe jako „waluta" związana z uczestnictwem w mediach społecznościowych [w:] K. Chałubińska-Jentkiewicz (red.), M. Nowikowska (red.), K. Wąsowski (red.), *Media w erze cyfrowej. Wyzwania i zagrożenia,* Wolters Kluwer, Warszawa 2021, s. 227 i nast.
[248] *password harvesting fishing*
[249] Szerzej: J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Uniwersytet w Białymstoku, Białystok 2017

majątkowej, zazwyczaj podszywa się (za pośrednictwem telefonu, adresu poczty elektronicznej lub strony internetowej) za jakąś instytucję, w tym instytucje bankowe[250]. Na bazie przytoczonych zagadnień teoretycznych, istnieje doskonała możliwość do płynnego przejścia i przeanalizowania sfery praktycznej tego typu przestępstw, koncentrując się na sposobie działania sprawcy, jego profilu, jak również sposobu wykorzystania w przestępczym procederze nowych technologii.

W 2021 r. odnotowano ogromny wzrost przestępstw wykorzystujących wyżej opisany proceder. Oszustwa polegające na podszywaniu się pod pracowników banku stały się niemalże plagą, co w konsekwencji doprowadziło do tego, że oszukanych w ten sposób było wiele osób, natomiast wartość wyrządzonej w ten sposób szkody określić można byłoby nawet mianem gigantycznej. Przestępstwo podszycia się za pracownika banku wymaga szczególnej uwagi i ocenić je należy wybitnie krytycznie, z uwagi na niejako zaburzanie zaufania obywateli do istotnych instytucji, w tym zwłaszcza instytucji bankowej. Wiele ludzi przechowując swoje środki na rachunkach bankowych, których są dysponentami we właściwych bankach, zawierzają, iż ich nierzadko oszczędności życiowe są bezpieczne i nie muszą się martwić o ich los. W zasadzie powszechnie przyjmuje się, iż ulokowanie środków na rachunkach bankowych jest najbezpieczniejszym rozwiązaniem z dotychczas możliwych, w związku z czym sprawcy podszywając się pod pracowników banku wykorzystują tę okoliczność i motywy klientów banku w celu wyrządzenia im szkody majątkowej[251].

Nie bez powodu ten typ cyberprzestępstwa analizowany jest bezpośrednio po przestępstwie oszustwa metodą „na wnuczka", albowiem przejawiają one wiele podobieństw różniąc się istotnym aspektem, tj. podszyciem się pod pracownika banku, ewentualnie innej instytucji zaufania publicznego. W przypadku tego typu przestępstwa, analogicznie jak poprzednio omawianym przypadku mamy do czynienia z podstawową formą przestępstwa oszustwa stypizowanego w art. 286 § 1 k.k., którego znamiona zostały wyczerpująco wyżej omówione, zatem bezcelowe jest ich omawianie po raz kolejny. Nadto podobnie jak w wyżej opisywanej praktyce przestępczego procederu podstawowym środkiem komunikacji elektronicznej wykorzystywanym przez sprawcę lub sprawców są połączenia głosowe wykonywane za pomocą telefonów, ewentualnie innych środków wykorzystujących

[250] A. Krasuski, A. Wolska-Bagińska, O. Zienkiewicz-Będźmirowska, *Działania naruszające prawa do domen internetowych*, Wolters Kluwer, 2021, s. 61 i nast.
[251] Szerzej: B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), *Prawo sztucznej inteligencji i nowych technologii 2*, Wolters Kluwer, Warszawa 2022

komunikację na odległość. Charakterystycznym elementem przestępstwa tego rodzaju jest nowatorska technika tzw. spoofingu numeru telefonu. Przyjąć można, iż technika ta fundamentalnie przejawia podobieństwa do korzystania z techniki ukrywania numeru telefonu poprzez jego zastrzeganie, niemniej jednak jest ona znacznie bardziej udoskonalona, rozwinięta i opierająca się na zdecydowanie nowszych metodach technologicznych aniżeli poprzednia, wymagając przy swoim funkcjonowaniu bardziej rozwiniętych technologicznie czynników, w tym zwłaszcza nowych technologii. Technika tzw. spoofingu numeru telefonu polega na wykorzystaniu przez sprawcę takich rozwiązań technicznych i technologicznych, które w konsekwencji doprowadzą do takich modyfikacji w wykorzystanym numerze telefonu, że na urządzeniu końcowym, czyli aparacie telefonu potencjalnego pokrzywdzonego numer MSDISM wykorzystany przez sprawcę podczas połączenia wyświetli się jako numer – w tym przypadku – banku[252]. Taki zabieg z pewnością w zdecydowanej większości przypadków wzmacnia stosowaną przez sprawców technikę manipulacji[253], skutecznie działają nawet wśród najbardziej czujnych klientów banku. Pokrzywdzony nawiązując połączenie głosowe jest w zasadzie stuprocentowo pewny, iż inicjującym połączenie jest pracownik banku. Odczucie to dodatkowo potęguje sposób rozpoczęcia rzeczonej rozmowy, gdzie sprawca celem zwiększenia swojej wiarygodności, przedstawia się jako pracownik techniczny lub pracownik działu IT konkretnej instytucji bankowej.

Sprawca, po zyskaniu zaufania pokrzywdzonego, co do zasady przedstawia mu różnego rodzaju historie, w zasadzie najczęściej dotyczące numeru rachunku bankowego prowadzonego na rzecz pokrzywdzonego w danym banku. Przykładów w tym zakresie w praktyce jest mnóstwo, m.in. sprawca wskazuje, iż z rachunku pokrzywdzonego doszło do nieautoryzowanej transakcji na znaczną sumę pieniędzy lub że podejmowane są próby zaciągnięcia pożyczki na dane pokrzywdzonego bądź iż doszło do przełamania zabezpieczeń informatycznych w postaci loginu i hasła do jego bankowości elektronicznej. Niezależnie od sposobu wprowadzenia pokrzywdzonego w błąd i niezależnie od stopnia skomplikowania przedstawionej mu historii, cel i zamiar działania sprawcy cyberprzestępstwa tego typu jest taki sam. Oczywiście, pośrednio i docelowo, działanie sprawcy ukierunkowane jest na osiągnięcie zysku, czyli doprowadzenia pokrzywdzonego do niekorzystnego rozporządzenia mieniem. Niemniej

[252] Szerzej: A. Krasuski , *Prawa i obowiązki abonentów usług telekomunikacyjnych*, Wolters Kluwer, Warszawa 2021

[253] K. Gurak, *Postęp techniczny i wynikająca z niego cyberprzestępczość jako wyzwanie współczesnej kryminologii* [w:] D. Dajnowicz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E.W. Pływaczewski (red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku,* 2022

jednak pierwszy etap przestępczego procederu nastawiony jest na wyłudzenie wysoko wrażliwych danych[254], najczęściej w postaci loginu i hasła do bankowości elektronicznej, co z kolei „otwiera" sprawcom całe spektrum działań, po uprzednim uzyskaniu dostępu do konta, m.in. wykonanie szeregu nieautoryzowanych transakcji finansowych, a w konsekwencji pozbawienie pokrzywdzonego wszystkich oszczędności, które przechowywał na danym rachunku bankowym. Sprawca, po nawiązaniu połączenia, informuje, iż dla celów zwiększenia bezpieczeństwa lub w celu wstrzymania wykonania nieautoryzowanej transakcji niezbędne jest podanie danych w postaci loginu i hasła do interfejsu bankowości elektronicznej, czy też zabezpieczeń w postaci jednorazowych kodów sms wysyłanych na telefon pokrzywdzonego. Wprowadzeni w błąd pokrzywdzeni, chcąc zapewnić maksymalną ochronę zgromadzonych przez siebie środków, pełni zaufania do osoby dzwoniącej, która podszyła się za pracownika działu technicznego banku, w zasadzie – niestety – bez zastanowienia podają pełen wachlarz wszelkich zabezpieczeń do swojej bankowości elektronicznej.

Co do zasady model działania sprawców wygląda niemal identycznie i po właściwym wykorzystaniu techniki spoofingu oraz technik manipulacyjnych, sprawca informuje, iż klient banku został ofiarą przestępstwa, a wyłącznie pomoc z działu technicznego lub działu IT zapewni ochronę jego interesów, a zwłaszcza jego mienia w postaci środków finansowych zgromadzonych na prowadzonym na jego rzecz rachunku bankowym. Wielokrotnie w celu wzmocnienia swojej autentyczności oraz wzmocnienia wiarygodności przedstawionej przez sprawcę historii, fałszywy pracownik banku informuje klienta banku, iż za chwile skontaktuje się z nim właściwy pracownik banku, który pomoże mu rozwiązać krytyczną sytuację, co oczywiście po chwili się dzieje – również przy wykorzystaniu techniki spoofingu. Przyjmując, iż pokrzywdzony chcąc zachować maksymalne reguły należytej ostrożności podejmuje czynności zmierzające do weryfikacji numeru abonenta, który inicjuje rzeczone połączenie głosowe, w tym m.in. sprawdza czy numer faktycznie należy do instytucji bankowej poprzez stronę internetową banku – dzięki uprzednio wykorzystanej przez sprawcę wyżej opisanej technice – uzyskuje potwierdzenie w tym zakresie, utwierdzając się w przekonaniu, iż rozmówca jest w rzeczywistości pracownikiem banku. Nic bardziej mylnego, w rzeczywistości jest to cyberoszust, którego działanie ma charakter *stricte* instrumentalny i nastawione jest na wyłudzenie danych od rzekomego klienta banku[255].

[254] Szerzej: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym kompiuterowym i systemom informatycznym*, Wolters Kluwer, 2016, s. 107

[255] Szerzej: W. Filipkowski (red.), E.W. Pływaczewski (red.), Z. Rau (red.), *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne,* Wolters Kluwer, 2015

Stopień działania sprawcy w przypadku tego typu przestępstwa jest nieco bardziej zaawansowany aniżeli w przypadku poprzednio opisywanego cyberprzestępstwa, głównie z powodu zastosowanej techniki, ale oczywiście nie tylko. W przypadku poprzedniego wyłudzenia, sprawca bezpośrednio uzyskiwał pieniądze od pokrzywdzonego, nie wykonując w zasadzie innych czynności „sprawczych" aniżeli wykonanie połączenia oraz zlecenie odbioru wyłudzonych środków. *Modus operandi* sprawcy w analizowanym typie przestępstwa wygląda nieco inaczej, albowiem na skutek zainicjowanego połączenia, sprawca bądź sprawcy uzyskują „wyłącznie" dane w postaci loginu i hasła do interfejsu bankowości elektronicznej i na tej podstawie dopiero podejmują konkretne czynności mające na celu rzeczywiste uzyskanie korzyści majątkowej[256]. Jak powszechnie wiadomo, obecnie – na skutek rozwoju technologicznego i nieustannego postępu w tym zakresie, co widoczne jest również w działalności instytucji bankowych – za pomocą bankowości elektronicznej przypisanej indywidualnie do określonego rachunku bankowego, można rozporządzić środkami finansowymi oraz zlecić dyspozycje w tym zakresie z poziomu telefonu czy komputera, ewentualnie innego urządzenia elektronicznego, bez konieczności wizyty w placówce banku. Zatem sprawca po uprzednim wyłudzeniu takich danych ma możliwość wytransferowania środków z rachunku bankowego należącego do pokrzywdzonego w ciągu kilku sekund, ale również w zasięgu jego możliwości jest chociażby zawarcie umowy pożyczki bez dodatkowego potwierdzenia i autoryzacji właściwego dysponenta rachunku bankowego. Powyżej przytoczone okoliczności jednoznacznie wskazują, iż szkoda majątkowa jaka powstaje na skutek przestępczego procederu, ma zdecydowanie większy zasięg aniżeli w przypadku pierwszego typu przestępstwa. Oczywiście takie zestawienia mogą wyglądać odmiennie w przypadku analizy konkretnych przypadków i wówczas te liczby mogą być inne i doprowadzać do przeciwnych wniosków, niemniej jednak nadal pozostaje to oceniane w granicach wyjątku.

Niejako przy okazji wspomnienia o dokonaniu nieautoryzowanych płatności z rachunku bankowego należącego do pokrzywdzonego, na skutek których dochodzi do wytransferowania środków pieniężnych wspomnieć należy o stosunkowo nowej metodzie płatności, która – z punktu widzenia cyberbezpieczeństwa – przejawia szereg „nieprawidłowości". Najczęściej środki należące do pokrzywdzonego dokonywane są właśnie za pomocą rzeczonej metody płatności, niemniej jednak zdarzają się również sytuacje, gdzie środki te przetransferowywane

[256] G. Lugano, M. Hudák, M. Ivančo, T. Loveček, *From the Mind to the Cloud: Personal Data in the Age of the Internet of Things* [w:] *AI Love you*, red. Y. Zhou, M.H. Fischer, Cham 2019

są inne numery rachunków bankowych, ale wówczas sytuacja z perspektywy organów ścigania jest nieco bardziej klarowna. Jeśli chodzi o „niedoskonałą" metodę płatności jest to tzw. BLIK, czyli system płatności mobilnych uruchomiony 9 lutego 2015 przez sześć polskich banków. Umożliwia użytkownikom smartfonów dokonywanie płatności bezgotówkowych w sklepach stacjonarnych i internetowych, wypłacanie i wpłacanie gotówki w bankomatach oraz dokonywanie przelewów i generowanie czeków z cyfrowym kodem[257].

Pojawienie się tego modelu płatności, przy wykorzystaniu usług mobilnych, jest kolejnym czynnikiem wskazującym na ogromny postęp technologiczny i fakt, iż nowe technologie w sposób zdecydowany ułatwiają działalność wielu sektorów i sfer życia społecznego[258]. Niemniej jednak pokazuje to również jak wiele niebezpieczeństwa, zwłaszcza z punktu widzenia cyberprzestępczości, niesie za sobą powstawanie nowych rozwiązań technologicznych. Sposobów wykorzystania przedmiotowego modelu płatności mobilnych jest bardzo wiele, niemniej jednak celowe i pełni uzasadnione jest ich przedstawianie w powiązaniu z konkretnymi przykładami przy okazji przedstawiania typów przestępstw. Wówczas faktyczne możliwości i ewentualne defekty zostaną przedstawione w sposób najbardziej czytelny, a przede wszystkim zrozumiały z praktycznego punktu widzenia.

W tym przypadku wskazać należy, iż sprawca po wyłudzeniu danych dotyczących logowania do bankowości elektronicznej, dokonuje transferu środków z rachunku bankowego należącego do pokrzywdzonego, najczęściej za pomocą transakcji BLIK, wykorzystując ją do wypłaty rzeczonych środków z dowolnego bankomatu w kraju czy też na świecie. W tym celu z aplikacji bankowości elektronicznej generowany jest sześciocyfrowy kod, który wpisywany jest w dowolnym bankomacie, po uprzednim wprowadzeniu żądania w zakresie zamiaru wypłacenia konkretnej kwoty pieniędzy, a następnie wymagane jest zatwierdzenie transakcji z poziomu właśnie aplikacji mobilnej, a skoro sprawca posiada do niej dostęp – cały zabieg trwa zaledwie kilka sekund i bankomat wypłaca pieniądze osobie w rzeczywistości nieuprawnionej. Wyżej wspomniano o negatywnych konsekwencjach płatności BLIK z punktu cyberbezpieczeństwa. Problematyka z tym związana dotyczy przede wszystkim tego, iż wówczas w historii transakcji konkretnego rachunku bankowego nie figurują żadne precyzyjne informacje dotyczące tego transferu, a jedynie wzmianka, iż jest to wypłata BLIK. Okoliczność ta niemalże w zupełności pozbawia organy ścigania możliwości ustalenia na rzecz kogo zostały

[257] Szerzej: A. Kaźmierczyk (red.), K. Michałowska (red.) M. Szaraniec (red.), *Verba volant, scripta mandet. Księga jubileuszowa dedykowana Pani Profesor Bogusławie Gneli,* 2023
[258] Szerzej: J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Uniwersytet w Białymstoku, Białystok 2017

przekazane te środki, a w konsekwencji – kto w rzeczywistości jest sprawcą przestępstwa. W przypadku przekazania środków na inny rachunek bankowy, w wykazie dokonanych transakcji co do zasady zawsze wskazana jest informacja na rzecz kogo środki zostały przekazane, w tym na jaki numer rachunku bankowego, zaś w tym przypadku brak jest jakiekolwiek punktu zaczepienia oprócz adresu bankomatu, z którego doszło do wypłacenia gotówki. Wydawać mogłoby się, iż wówczas po stronie organów ścigania generuje się możliwość uzyskania nagrań z monitoringu a w konsekwencji sporządzenia rysopisu sprawcy. Nic bardziej mylnego, kamery monitoringu w bankomatach są skierowane w taki sposób, iż bardzo łatwo sprawcy zasłonić twarz, chociażby za pomocą czapki z daszkiem, a mając na względzie często fakt, iż cyberprzestępstwa nie są popełniane przez przypadkowych sprawców, jest to dla nich łatwe do „pokonania". Nadto pokrzywdzeni wielokrotnie zawiadamiają o popełnionych na ich szkodę przestępstwach, często z dużym opóźnieniem, co z punktu widzenia faktu, iż nagrania z monitoringów bankomatów są niezwykle szybko nadpisywane, generuje kolejną przeszkodę po stronie organów ścigania w celu wykrycia sprawcy przestępstwa[259].

Pokrzywdzony dowiaduje się o tym, iż został ofiarą przestępstwa co do zasady bardzo szybko, albowiem po zalogowaniu się do swojej bankowości elektronicznej okazuje się, że z jego rachunku bankowego wytransferowano środki finansowe. O ewentualnej umowie pożyczki zawartej na jego dane, dowie się jednak znacznie później. Zazwyczaj w przypadku uzyskania pisemnego wezwania do uregulowania zadłużenia lub co więcej – dopiero w momencie uzyskania tytułu wykonawczego wydanego przez sąd. Kwestia ta poddana zostanie dokładnej analizie na tle kolejnych typów przestępstw, niemniej jednak w tym miejscu zasygnalizować należy, iż w przypadku wykorzystania danych pokrzywdzonego w ostatni z opisanych sposobów i wzięcia pożyczki gotówkowej na jego dane, modyfikacji ulega ocena prawnokarna czynu. W takim przypadku niezbędne jest uwzględnienie w kwalifikacji prawnej przestępstwa tzw. podszycia się, czyli wykorzystania m.in. cudzych danych osobowych w celu wyrządzenia pokrzywdzonemu szkody majątkowej lub osobistej, a następnie posłużenie się tymi danymi jako własnymi. Przestępstwo to stypizowane jest w art. 190a § 2 k.k. i zgodnie z treścią aktualnie obowiązujących przepisów kodeksu postępowania karnego, wymaga się, aby postępowanie przygotowawcze w tym zakresie prowadzone było w formie śledztwa. Niemniej

[259] Brak jest regulacji prawnych odnoszących się do obowiązkowego okresu przechowywania zapisu nagrań z monitoringu, niemniej jednak praktyka wskazuje, iż okres ten wynosi około 1 miesiąca

jednak, szczegółowa analiza tego typu przestępstwa zostanie przedstawiona podczas omawiania kolejnego typu cyberprzestępstwa.

Bezpośrednio przy okazji analizy sposobu działania sprawcy tego typu przestępstwa, nie sposób również nie wspomnieć o bardzo często wykorzystywanej technice, która swoją działalność zawdzięcza nowym technologiom. W przypadku omawianego typu przestępstwa ta technika zaczęła być wykorzystywana w większości przypadków dopiero w 2021 r., niemniej jednak na przestępczym rynku znała była już znacznie wcześniej. Zaznaczyć jednoznacznie należy, iż ten sposób działania sprawcy lub sprawców nie jest praktykowany każdorazowo, a tylko w niektórych przypadkach. Kwestia ta dotyczy złośliwego oprogramowania instalowanego zdalnie na telefonie należącym do pokrzywdzonego, czyli malware**,** które jest swoistego rodzaju oprogramowaniem, któremu należy przypisać przymiot złośliwego, albowiem jego zainstalowanie może doprowadzić do zainfekowania używanego urządzenia elektronicznego[260]. Jego celem jest pozyskanie w sposób nielegalny różnego rodzaju danych, w tym również danych do logowania do bankowości elektronicznej. Sprawca co do zasady przesyła „ofierze" adres strony internetowej, wprowadzając jednocześnie go w błąd co do rzeczywistego celu, po czym pokrzywdzony wchodząc w przesłaną stronę nieświadomie instaluje na swoim komputerze czy też smartfonie złośliwe oprogramowanie, które pozwala sprawcy na dokładne szpiegowanie swojej ofiary, uzyskując dostęp do wszystkich danych.

Wyżej opisany sposób działania sprawcy, oparty na funkcjonowaniu oprogramowania zwanego szpiegowskim pozwala na uzyskanie – w nieco bardziej złożony sposób – danych, na których sprawcom najbardziej zależy. Uzyskując dostęp do ekranu i zasobów telefonu, komputera czy też innego urządzenia wykorzystywanego przez pokrzywdzonego, sprawca uzyskuje bezpośredni dostęp do wszystkich haseł i loginów, w tym również do danych dotyczących logowania do interfejsu bankowości elektronicznej – co w przypadku tego typu przestępstwa – było jego celem[261]. Co do zasady w celu zainstalowania przez pokrzywdzonego złośliwego oprogramowania, sprawca podczas prowadzonej rozmowy głosowej wskazuje mu na konieczność zainstalowania aplikacji, która pomoże przywrócić bezpieczeństwo na należącym do niego rachunku bankowym czy też pozwoli na przerwanie nieautoryzowanych transakcji (w zależności od uprzednio przedstawionej historii). Pokrzywdzony, z uwagi na swoje krytyczne położenie, obawę i strach przed utratą oszczędności całego życia, a także

[260] Szerzej: J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Uniwersytet w Białymstoku, Białystok 2017
[261] Szerzej: M. Domagała, *Prawnokarna ochrona prywatności użytkowników Internetu,* Państwo i Prawo 2010/3/75-86

w poczuciu zaufania do rzekomego pracownika banku, wykona niemalże każde polecenie i „sugestię" rozmówcy. Wówczas świadomie pobiera na swój telefon złośliwe oprogramowanie najczęściej mające postać programu AnyDesk lub Quicksupport, a po prawidłowym zalogowaniu, sprawca „sparowuje" się z telefonem pokrzywdzonego i w zasadzie wówczas osiąga cel swojej przestępczej działalności, albowiem faktyczne doprowadzenie do niekorzystnego rozporządzenia mieniem jest już wyłącznie formalnością[262].

1.2.3. Oszustwa na platformach sprzedażowych i portalach społecznościowych

W praktyce przyjmuje się, że oszustwa popełniane za pośrednictwem sieci teleinformatycznej przy wykorzystaniu internetowych platform sprzedażowych oraz portali społecznościowych są najbardziej popularnymi cyberprzestępstwami. W zakresie platform sprzedażowych wskazać należy, iż aktualnie najpopularniejszą jest Olx.pl oraz – rzadziej – Allegro.pl. W działalności sprawców wykorzystywana jest również stosunkowo nowa platforma, która bezpośrednio łączy się z działalnością portali społecznościowych, czyli tzw. Marketplace obsługiwane przez Facebook. Jest to swoistego rodzaju witryna, na której użytkownicy portalu społecznościowego Facebook wystawiają oferty sprzedaży różnych przedmiotów. Natomiast w zakresie portali społecznościowych, sprawcy dla celów przestępczych wykorzystują najbardziej popularne portale, zatem nie ma wątpliwości co do tego, iż najczęściej przestępstwa popełniane są za pośrednictwem Facebooka oraz – obsługiwanego przez tego samego administratora – komunikatora społecznościowego Messenger, który ściśle współpracuje i związany jest z konkretnym kontem użytkownika na portalu społecznościowym Facebook.

Skoro skonkretyzowano już wiedzę na temat tego, jakie platformy sprzedażowe oraz jakie portale społecznościowe wykorzystywane są w celu popełnienia tego typu przestępstwa oszustwa, bezpośrednio można przejść do rozważań dotyczących sposobu działania sprawców w tym przypadku, które w odniesieniu do poprzednio opisywanych działań, które miały charakter złożony i skomplikowany, ten nie bez powodu ocenić należy jako podstawowy.

W pierwszej kolejności analizie poddać należy przestępstwa oszustwa popełniane przy wykorzystaniu platform sprzedażowych, tj. m.in. Allegro czy Olx.pl, które aktualnie są najbardziej popularnymi miejscami w sferze Internetu, gdzie sprawcy w bardzo łatwy sposób oszukują pokrzywdzonych. Praktyka oraz sposób działania sprawców jest zakorzeniony

[262] Por. Wyrok Sądu Rejonowego w Chełmnie z dnia 18 kwietnia 2023 r. sygn. I C 433/21, LEX nr 3574487

w samym schyłku popularności przestępstw popełnianych za pośrednictwem sieci teleinformatycznej. Ten typ oszustwa niejako zapoczątkował cyberprzestępstwa jako takie ogólnie. *Modus operandi* sprawcy można podzielić na kilka etapów, przy czym pierwszy co do zasady polega na umieszczeniu ogłoszenia sprzedaży jakiegoś przedmiotu właśnie na platformie sprzedażowej, najczęściej za znacznie korzystniejszą cenę aniżeli inne ogłoszenia dotyczące tych samych przedmiotów. Zainteresowany wyjątkowo opłacalną ofertą klient, kontaktuje się za pośrednictwem danej platformy sprzedażowej ze sprawcą celem uzgodnienia wszelkich szczegółów dotyczących zapłaty za towar oraz jego wysyłki. W związku z tym, iż powszechnie przyjętą metodą płatności za zakupy dokonywane przez Internet jest przedpłata, czyli dokonanie przelewu na rachunek bankowy podany przez sprzedającego zanim nada on przesyłkę, której przedmiotem jest zakupiony towar, sprawca oraz pokrzywdzony najczęściej po negocjacjach uzgadniają właśnie tę formę zapłaty. Znaczny wzrost popularności dokonywania zakupów za pośrednictwem Internetu, który niemalże podwoił się w czasach, w których ogłoszono pandemię w Polsce i na świecie, bezpośrednio spowodował wzrost cyberprzestępstw popełnianych w ten sposób. Sposób działania sprawcy, nie wzbudza u choćby najbardziej czujnego klienta żadnych wątpliwości, albowiem – jak wyżej wskazano – odnotowany wzrost popularności dokonywania zakupów w ten sposób, a także upowszechniona praktyka dokonywania płatności metodą przedpłaty stwarza idealne zaplecze dla przestępczych procederów.

Kolejnym etapem omawianego typu przestępstwa jest dokonanie transferu środków przez pokrzywdzonego na uprzednio wskazany przez sprawcę numer rachunku bankowego. Pokrzywdzony po uprzednim wygenerowaniu z bankowości elektronicznej potwierdzenia wykonania przelewu, przesyła je sprzedającemu oczekując bezzwłocznej przesyłki. Oczekiwanie zazwyczaj bywa długotrwałe i finalnie okazuje się, że przesyłka z zamówionym towarem nie zostaje doręczona pokrzywdzonemu, a kontakt ze sprzedającym – zarówno za pośrednictwem platformy sprzedażowej jak również za pośrednictwem podanego przez niego uprzednio numeru – aktualnie jest w zasadzie niemożliwy. Jak przedstawiono, co do zasady sposób działania sprawcy nie jest skomplikowany, a cała czynność sprawcza polega w pierwszej kolejności na umieszczeniu oferty sprzedaży na właściwej platformie, następnie skuteczne nawiązanie kontaktu z potencjalnym klientem i w konsekwencji otrzymanie od niego ustalonej w wyniku negocjacji kwoty pieniężnej. Analogicznie jak w przypadku pozostałych typów cyberprzestępstw omawianych w rzeczonym rozdziale, opisywany sposób działania sprawcy wyczerpuje znamiona przestępstwa oszustwa spenalizowanego w art. 286 § 1 kodeksu

karnego, które to znamiona zostały wyczerpująco uprzednio omówione. W zakresie wprowadzenia w błąd pokrzywdzonego przez sprawcę podkreślić jedynie należy, iż odnosi się to najczęściej zarówno do faktu posiadania przez sprawcę rzeczy będącej przedmiotem oferty sprzedaży jak również co do możliwości oraz zamiaru wywiązania się z zawartej umowy sprzedaży.

Przedpłata jako metoda płatności wykorzystywana jest najczęściej wśród przestępstw tego rodzaju, aczkolwiek nie jest to jedyna metoda płatności. Bardziej czujni klienci, chcąc zakupić towar za pośrednictwem Internetu i jednocześnie zachować wszelkie reguły ostrożności mające na celu uchronienie ich przed potencjalnymi oszustami, decydują się na formę płatności przy odbiorze. Zabezpiecza to klientów przed bezpodstawnym przesłaniem ustalonej ceny na rzecz sprzedającego, który finalnie nie przesłałby zamówionego towaru. Jednakże czy faktycznie takie działanie „ochronne" pokrzywdzonego spełnia w rzeczywistości walor zabezpieczającego jego interesy? Nic bardziej mylnego. Oczywiście, w przeciwieństwie do poprzednio opisanej wersji i sposobu działania sprawcy, w tym przypadku w celu uzyskania środków finansowych tytułem ceny za zamówiony towar, nada on na uprzednio wskazany przez pokrzywdzonego adres, przesyłkę najczęściej za pośrednictwem firmy kurierskiej, ale nierzadko również za pośrednictwem operatora pocztowego. Pokrzywdzony, który uprzednio – w jego ocenie – dochował wszelkich reguł ostrożności, w chwili otrzymania zamówionej przesyłki o uprzednio przyświecających mu zasadach zupełnie zapomina. Po pokwitowaniu odbioru, kupujący uiszcza kurierowi lub listonoszowi uprzednio umówioną ze sprzedającym kwotę tytułem ceny, bez uprzedniego zapoznania się z zawartością przesyłki. Ku jego zdziwieniu i zaskoczeniu, zawartość przesyłki jest skrajnie odmienna od zamówionego przedmiotu, w tym np. w postaci telefonu czy też innego sprzętu elektronicznego. Najczęściej przedmiotem przesyłki jest zupełnie bezwartościowy przedmiot. Jak widać, w zasadzie sposób działania sprawcy wygląda analogicznie jak w poprzednio opisanej wersji, niemniej jednak dostosowany został niejako do sposobu płatności uzgodnionego pomiędzy stronami transakcji, sposób wprowadzenia pokrzywdzonego w błąd przedstawia się analogicznie, albowiem sprawca w rzeczywistości nie posiadał przedmiotu, który *de facto* sprzedał, jak również nie miał zamiaru i możliwości wywiązania się z zawartej umowy sprzedaży. Jedyna subtelna różnica sprowadza się do tego, że w drugiej z opisywanych wersji sprawca zmuszony był do wysłania jakiejkolwiek przesyłki pokrzywdzonemu oraz poczynienia nakładów finansowych w tym zakresie, które w rzeczywistości jednak stanowią setną część środków, które w rzeczywistości uzyskał na skutek przestępczego działania.

W zakresie nowych technologii wykorzystanych przez sprawcę w tego rodzaju przestępstwach co do zasady jest to wyłącznie zarejestrowanie konta użytkownika na odpowiedniej platformie sprzedażowej. Niemniej jednak jak wyżej wielokrotnie wskazywano, każde działanie sprawcy w sieci zostawia po sobie ślady, które następnie umożliwiają organom ścigania ustalenie jego tożsamości. W tym przypadku, w celach rejestracyjnych, sprawca podaje adres poczty elektronicznej, numer telefonu. Nie sposób zapomnieć również o adresie IP, którym posługuje się sprawca przy każdorazowym ruchu w sieci. Nadto niezależnie od przyjętego sposobu płatności za zamówiony towar, środki finansowe zostają przetransferowane na konkretny numer rachunku bankowego sprawcy, które umożliwia organom ścigania procesowe pozyskanie kolejnych danych umożliwiających zidentyfikowanie sprawcy przestępstwa. Analogicznie, jak w poprzednich przypadkach, algorytm działania organów ścigania oraz sposób procesowego zabezpieczenia danych retencyjnych zostanie omówiony w kolejnej części pracy.

Po poddaniu dokładnej i szczegółowej analizie przestępstwa oszustwa popełnionego przy wykorzystaniu platform sprzedażowych, krótko należy omówić również kolejny rodzaj cyberprzestępstwa, tj. przestępczy sposób działania sprawców wykorzystujących portale społecznościowe, których opis jest niezwykle bardzo zbliżony do uprzednio opisywanego *modus operandi*, będące często w ścisłym powiązaniu. Całokształt danych i informacji przedstawianych w powiązaniu z konkretnymi przykładami w zasadzie jednoznacznie wskazuje, iż rozwój nowych technologii wywiera bezpośredni wpływ na cyberbezpieczeństwo. W związku z nieustannie i bardzo dynamicznie rosnącą popularnością mediów społecznościowych, stały się one niemalże doskonałym środowiskiem dla cyberprzestępców. Powtarzając wskazane na wstępie przedmiotowej rozprawy dane statystyczne, wykazujące nieprawdopodobnie szokujące liczby przedstawione przez najnowszy raport Hootsuit wskazać należy, iż mediów społecznościowych używa aktualnie 25,9 mln osób**,** a to zdecydowanie więcej niż połowa (68.5%) populacji naszego kraju (37,82 miliona osób). Porównując te dane z wynikami ubiegłorocznymi, wzrost wynosi aż 2,5 miliona (11%) w stosunku do roku poprzedniego. Nie sposób więc uniknąć stwierdzenia, iż wzrost użytkowników portalów społecznościowych wywiera bezpośredni wpływ na liczbę cyberprzestępstw popełnianych w ten sposób.

Media społecznościowe, w praktyce najczęściej portal społecznościowy Facebook administrowany przez zagranicznego operatora, wykorzystywane są przez sprawców nie tylko jako platforma sprzedażowa w celu popełnienia poprzednio opisanego przestępstwa oszustwa.

Wyraźnie zaznaczyć należy, iż portale społecznościowe bezpośrednio związane są z komunikatorami społecznościowymi, wśród których zdecydowany prym wiedzie komunikator Messenger, który obok komunikatora WhatsApp stał się podstawową formą komunikacji międzyludzkiej w wymiarze elektronicznym i komunikacji na odległość, w części zastępując swoją funkcjonalnością uprzednio najbardziej popularne wiadomości tekstowe SMS. Konwersowanie za pośrednictwem komunikatorów społecznościowych jest w zasadzie bezpłatne, wymaga wyłącznie dostępu do sieci Internetowej, natomiast wysyłane wiadomości dochodzą do odbiorcy co do zasady niezwłocznie po ich wysłaniu, niezależnie od miejsca na świecie, w którym się aktualnie znajdują rozmówcy. Wzrost popularności w tym zakresie bezpośrednio wpłynął na ukształtowanie się kolejnej nielegalnej praktyki cyberprzestępców.

Sposób działania sprawcy w przypadku omawianego typu oszustwa jest nieco bardziej skomplikowany aniżeli w poprzednio omawianej wersji i wymaga ze strony oszusta większego zaangażowania, albowiem w tym przypadku instrumentalne działanie sprawcy nastawione na osiągnięcie korzyści majątkowej wymaga uprzedniego przełamania zabezpieczeń informatycznych w postaci loginu i hasła do konta użytkownika na portalu społecznościowym, a tym samym do powiązanego z nim komunikatora. Uzyskując dostęp do takiego konta, sprawca uzyskuje również dostęp do „książki rozmówców" oraz do historii rozmów. W zasadzie bez większego wysiłku sprawca na tej podstawie może wytypować osoby z najbliższego otoczenia użytkownika, do konta którego uzyskał dostęp. *De facto* z punktu widzenia przestępstwa oszustwa, osoba ta nie uzyskuje statusu pokrzywdzonego w tym zakresie. Po wytypowaniu takich osób, sprawca podszywając się pod inną osobę, wprowadzając tym samym rozmówcę w błąd co do tożsamości osoby, z którą konwersuje, inicjuje rozmowę za pośrednictwem komunikatora społecznościowego. Praktyka wskazuje, iż rozmowa co do zasady przebiega w ten sposób, albowiem sprawca prosi rozmówcę o wygenerowanie kodów blik umożliwiających natychmiastową zapłatę za zamówiony towar czy też poczynione zakupy, co spowodowane ma być chwilowymi problemami z dostępem do własnej bankowości oraz zgromadzonych tam środków. W związku z nieustannie rosnącą popularnością mediów społecznościowych, regularnie upowszechnianą praktyką modelu natychmiastowych płatności BLIK jak również fakt, iż pokrzywdzony rozmówca jest przekonany, iż po drugiej stronie znajduje się osoba dla niego bliska, w zasadzie nie pojawiają się żadne wątpliwości co do autentyczności i wiarygodności, w związku z czym w znacznej większości przypadków te kody blik są faktycznie generowane i przesyłane osobie bliskiej (a w rzeczywistości sprawcy). Co bardziej zaskakujące, co do zasady, pokrzywdzony po

uprzednio otrzymanej prośbie, co najmniej dwukrotnie generuje taki kod, przy czym zazwyczaj każdy dotyczy kwoty co najmniej 1000 zł. W rzeczywistości środki te wypłacane są przez osoby współpracujące ze sprawcą za pośrednictwem bankomatów zazwyczaj znajdującym się nawet kilkaset kilometrów od miejscowości, w której zamieszkuje pokrzywdzony. Pokrzywdzony dowiaduje się o tym, iż padł ofiarą przestępstwa wówczas, kiedy prawdziwy rozmówca uzyska ponowny dostęp do swojego konta na portalu społecznościowym. Wówczas w historii rozmów dostrzega konwersacje, które w rzeczywistości nie były przez niego prowadzone.

Z dogmatycznego punktu widzenia oraz prawnokarnej oceny czynu wskazać należy, iż ten typ cyberprzestępstwa jest ciekawym i złożonym, albowiem w rzeczywistości sprawca swoim działaniem wyczerpuje znamiona dwóch przestępstw, przy czym każde z nich popełniane jest na szkodę innej osoby. W pierwszej kolejności sprawca swoim działaniem wyczerpuje znamiona przestępstwa stypizowanego w art. 267 § 1 k.k., albowiem sprawca nie będąc osobą uprawnioną uzyskuje dostęp do zbioru informacji zupełnie dla niego nieprzeznaczonej, uprzednio przełamując informatyczne zabezpieczenia do zbioru tych informacji, czyli do konta użytkownika[263]. Omawiany sposób działania sprawcy jest w zasadzie książkowym przykładem zrealizowania znamion przywołanego przestępstwa. Podkreślić jednakże należy, iż w tym przypadku sprawca działa na szkodę osoby, do konta której uzyskał nieuprawniony dostęp przełamując zabezpieczenia w postaci loginu i hasła. Szkoda finansowa co prawda w zasadzie nie powstała po jego stronie, niemniej jednak nie tylko taki wymiar szkody uzasadniania przypisanie komuś waloru i statusu pokrzywdzonego w postępowaniu karnym. Drugie przestępstwo z kolei ma wymiar typowego przestępstwa oszustwa stypizowanego w art. 286 § 1 k.k., którego znamiona precyzyjnie omówiono na tle poprzednich typów cyberprzestępstw. W tym przypadku sprawca działa natomiast klasycznie na szkodę osoby, którą doprowadził do niekorzystnego rozporządzenia mieniem wprowadzając ją w błąd co do tożsamości rozmówcy.

Wykorzystane przez sprawcę lub sprawców w celu popełnienia rzeczonego typu cyberprzestępstwa nowe technologie, w tym postaci przełamania zabezpieczeń do konta użytkowników w mediach społecznościowych, wybór natychmiastowego modelu płatności blik, działanie w ramach tzw. hackingu[264] w sposób bezpośredni implikuje konieczność

[263] Art. 267 § 1 k.k., M. Mozgawa (red.), *Kodeks karny, komentarz aktualizowany*, LEX, 2023

[264] Szerzej: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016; F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013/13

stwierdzenia, że mamy do czynienia z klasycznym przykładem cyberprzestępstwa, które dla swojego bytu wykorzystuje działalność nieustannie rozwijającej się sieci teleinformatycznej[265].

1.2.4. Kryptowaluty jako przedmiot przestępstwa

Rozwój nowych technologii i postęp technologiczny dyktuje warunki oraz powstanie czynników decydujących o możliwościach i sposobach popełniania przestępstw, w tym również cyberprzestępstw. Nie ma wątpliwości co do tego, iż widoczny wzrost zainteresowania jakąś dziedziną oznacza, że w danej sferze pojawi się skupisko wielu ludzi, a z uwagi na wzrost popularności niezbędne jest udoskonalanie obsługujących tą sferę systemów, co oczywiście wymaga nakładu pracy i czasu, na skutek czego powstają pewne elementy „niedoskonałości" otwierające sprawcom drogę do przestępstw, niejednokrotnie takich, którym można przypisać walor doskonałych.

Nie z przypadku ten rodzaj przestępstwa omawiany jest jako ostatni typ cyberprzestępstw objętych zakresem przedmiotowej rozprawy. Przemawia za tym wiele czynników. Po pierwsze wskazać należy, iż przestępstwo oszustwa metodą na bitcoina są stosunkowo nowym cyberprzestępstwem, a z pewnością najnowszym spośród w tym rozdziale omawianych. Nadto cyberprzestępcy dążąc do osiągnięcia korzyści majątkowej wykorzystują jednocześnie wiele, a zaryzykować można stwierdzeniem, iż nawet wszystkie dotychczas omówione techniki działania sprawców wykorzystujące nowe technologie. *Modus operandi* wobec tego, w tych przypadkach jest zdecydowanie bardziej skomplikowany, złożony, ale również nadal bardzo tajemniczy i zaskakujący. W związku z nowatorskimi metodami działania sprawców przestępstw tego rodzaju, wiele z wykorzystanych przez nich technik nadal nie jest zweryfikowanych, nawet dla organów ściągania, które nieustannie doskonalą algorytm działania mający na celu ustalenie sprawców przestępstw. Ten sposób działania sprawców pojawił się jako udoskonalony sposób oszustwa na wnuczka czy policjanta. Niemniej jednak w związku z nowatorskim charakterem przestępstwa, techniki wykorzystane przez sprawców opierają się na bycie i funkcjonalności najnowszych spośród dostępnych nowych technologii.

Na przestrzeni 2021 r. i 2022 r. niezwykle na popularności zyskała nowa metoda zarabiania pieniędzy i ich inwestowania odnosząca się do rynku giełdowego oraz rynku szeroko rozumianych kryptowalut[266]. Wskazuje się dla celów praktycznych, iż kryptowaluty to rozproszony system księgowy bazujący na kryptografii klucza publicznego, przechowujący

[265] R. Russell (red.), *Hack Proofing Your Network. Edycja Polska*, Gliwice 2002
[266] Szerzej: M. Marcinkowska, *Egzekucja komornicza z kryptowalut,* Przegląd Prawa Handlowego, 2021/6/12-16

informację o stanie posiadania w umownych jednostkach. Wśród cech kryptowalut wskazuje się na otwartość systemu, decentralizację, przejrzystość, pseudoanonimowość, nieodwracalność transakcji oraz brak uregulowań prawnych. Dla wykazania potęgi tego instrumentu, wskazać należy, iż w 2023 roku ilość bitcoinów (BTC) jako jednego z wielu rodzajów kryptowaluty, w obiegu wynosi ponad 19 400 000[267]. W Internecie, w tym na portalach społecznościowych, na stronach dotyczących możliwości zainwestowania środków finansowych, pojawia się ogromna liczba informacji dotycząca kryptowalut. Są to zazwyczaj niezwykle korzystne i opłacalne oferty zachęcające do ulokowania pieniędzy w precyzyjnie opisany sposób, obiecujące szybki i satysfakcjonujący zarobek. Po wpisaniu tego hasła w jedną z najbardziej popularnych przeglądarek internetowych Google, można dostrzec jak ogromną reklamą i zainteresowaniem cieszy się wspominany rynek[268]. Niezliczona ilość witryn internetowych, za pośrednictwem których można zainwestować pieniądze, oferty zakupu książek i poradników dotyczących „mądrego i przemyślanego" inwestowania w kryptowaluty, a także szereg odniesień wskazujących na nieustannie rosnący wzrost znaczenia tego środka płatności na giełdach rynków światowych. Nie ma wątpliwości co do tego, iż wizja szybkiego zysku oraz w zasadzie „bezwysiłkowego" zarobienia pieniędzy jest i była atrakcyjnym zwizualizowaniem własnej rzeczywistości, natomiast ludzie w obliczu możliwości zarobienia ogromnych pieniędzy, a w konsekwencji spektakularnej zmiany swojego życia niejako tracą obowiązek zachowania choćby podstawowych reguł ostrożności. Rzeczone odczucia wzmacnia dodatkowo fakt, iż niejednokrotnie wspomniany sposób inwestowania pieniędzy reklamowany jest przez bardzo popularne osoby, co dodatkowo wzmacnia poczucie zaufania do tego rynku wśród potencjalnych inwestorów.

Na to czym są kryptowaluty wskazuje już ich nazwa, która w sposób bezpośredni odnosi się do kryptografii. Nie ma wątpliwości co do tego, iż jest to jeden z rodzajów waluty, wyróżniający się od pozostałych bardzo specyficznym elementem, tj. faktem, iż istnieje ona wyłącznie w postaci cyfrowej[269]. Nie ma co prawda wymiaru materialnego, co absolutnie nie oznacza, iż nie ma żadnej wartości. Pomimo, iż kryptowaluty w zasadzie zamiennie określane

[267] https://www.coinbase.com/pl/price/bitcoin (dostęp: 10.07.2023 r.)

[268] M. Grzybkowski, S. Bentyn, Kryptowaluty. *Dlaczego jeden bitcoin wart będzie milion dolarów?*, Poznań 2018; szerzej: C.H. Kim, A. Kriwoluzky, *Public or Private? The Future of Money*, Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2019
https://www.europarl.europa.eu/cmsdata/207653/13.%20PE%20642.356%20DIW%20final%20publication-original.pdf (dostęp: 15.06.2023 r.)

[269] P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego,* Prokuratura i Prawo 2017/6/36-59

są mianem walut wirtualnych, mają one wymierną wartość materialną i za ich pomocą można uregulować płatności za różnego rodzaju towary i usługi[270]. Niemniej jednak aktualna pozycja kryptowalut na rynku w zasadzie wyraźnie wskazuje, że obecnie ich użytkownicy rzadko wykorzystują je jako środki płatności, zdecydowanie częściej postrzegane są one jako instrumenty finansowe, podlegające bieżącej i regularnej wycenie, umożliwiające uzyskanie zysku przy odpowiednim wykorzystaniu dostępnych urządzeń, instrumentów, wiedzy i obserwacji kursów kryptowalut[271]. Kryptowaluty, analogicznie jak każda inna waluta, posiadają dynamicznie zmieniające się kursy i rzetelna ich analiza daje szansę inwestującym na osiągnięcie spektakularnych zarobków. Sprzedaży i zakupu kryptowalut dokonuje się na giełdach, które bardzo przypominają tradycyjne giełdy akcji czy obligacji[272]. Wśród omawianego typu walut wyróżnia się kilka rodzajów, w tym najpopularniejszą kryptowalutę, czyli bitcoin. Powszechnie przyjmuje się, że to właśnie bitcoin (BTC) dał początek kryptowalutom i technologii blockchain[273]. Powstał na początku 2009 roku. Niemniej jednak analiza rynku kryptowalut oraz funkcjonowania tego systemu, jak również ściśle związanych z nim instrumentów i środków nie jest przedmiotem niniejszych rozważań, w związku z czym należy bezpośrednio przejść do analizy, w tym oceny prawnokarnej przestępstw oszustwa przy wykorzystaniu bitcoinów i rynku kryptowalut.

W pierwszej kolejności, zanim ocenie poddany zostanie prawnokarny aspekt czynów zabronionych, szczegółowo i dogłębnie przeanalizować należy sposób działania sprawców. Najczęściej punktem wyjścia omawianego przestępstwa i elementem początkowym jest znalezienie przez potencjalnego pokrzywdzonego oferty inwestowania na rynku kryptowalut, obiecującego niemalże natychmiastowy i wysoki zysk. Takie reklamy znajdowane są co do zasady w sieci teleinformatycznej, w tym również na portalach społecznościowych. Zaintrygowany szansą zarobienia obiecujących środków finansowych pokrzywdzony nawiązuje kontakt z brokerem obsługującym daną firmę zajmującą się „pomocą" w zarobku na kursie bitcoina czy innej kryptowaluty. Wówczas najczęściej wypełniają właściwy formularz, który bywa początkiem rzeczonej współpracy. Następnie, na podany przez sprawcę numer telefonu, kontaktuje się doradca deklarujący pomoc, przeprowadzający obszerną rozmowę na

[270] A. Behan, *Waluty wirtualne jako przedmiot przestępstwa,* Krakowski Instytut Prawa Karnego Fundacja, Kraków 2022, s. 580 i nast.
[271] Szerzej: M. Ahmed, I. Shumailov, R. Anderson, *Tendrils of Crime: Visualizing the Diffusion of Stolen Bitcoins*, w: *Graphical Models for Security*, red. G. Cybenko, D. Pym, B. Fila, Springer International Publishing 2018
[272] https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/?sh=5e10f64741a4 (dostęp: 10.07.2023 r.)
[273] Szerzej: J. Dąbrowska, *Charakter prawny bitcoin*, „Człowiek w Cyberprzestrzeni" 2017, nr 1

temat rynku kryptowalut, przedstawiający wyłącznie pozytywne aspekty jego działalności, zachęcający do zainwestowania w pierwszej kolejności niewielkiej kwoty pieniężnej. Przedstawione przez doradcę obietnice silnie wzmacniają w kliencie poczucie zaufania, bezpieczeństwa za chwilę ulokowanych środków oraz wiarę w możliwość zwiększenia swoich zasobów finansowych[274].

Praktyka wskazuje, iż zazwyczaj w pierwszej kolejności pokrzywdzeni inwestują pozornie niewielkie sumy pieniężne, dotyczące zazwyczaj wartości około 250 euro. Wówczas pokrzywdzeni, na prośbę i polecenie doradcy, instalują na swoim telefonie, komputerze czy też innym urządzeniu elektronicznym, którym się posługują, instalują aplikację i oprogramowanie szpiegowskie, najczęściej program AnyDesk, umożliwiający sprawcom zdalny dostęp do urządzenia pokrzywdzonego. Technika ta została wyczerpująco omówiona przy okazji poprzednio analizowanych typów cyberprzestępstw. Często celem wzmocnienia zaufania i wiarygodności pokrzywdzonego w zakresie bezpieczeństwa zainwestowanych przez niego środków, wykorzystując działanie oprogramowania szpiegowskiego, sprawca instaluje – za wiedzą i zgodą pokrzywdzonego – wszystkie potrzebne do inwestowania na rynku kryptowalut aplikacje, m.in. binance[275], portfolio czy revolut służący do wpłaty i wypłaty środków.

Dalszy etap działania sprawców sprowadza się do nieustannego bycia w kontakcie z pokrzywdzonym, regularnie przekazując mu cenne wskazówki i informacje dotyczące zainwestowanych przez niego środków. W pewnym momencie doradca podczas rozmowy z pokrzywdzonym wskazuje na nagłą możliwość zarobienia ogromnych pieniędzy i niecodzienną szansę dla inwestującego spowodowanym nagłym skokiem lub spadkiem na giełdzie kryptowalut. Żadnym zaskoczeniem nie jest to, że dla osiągnięcia obiecywanego zarobku, niezbędne jest zainwestowanie większej ilości pieniędzy. Wówczas pokrzywdzony w obliczu szansy zarobienia spektakularnych pieniędzy, niejednokrotnie „inwestuje" środki stanowiące dorobek jego życia lub co więcej zaciąga na ten cel kredyt lub pożyczkę.

Często przyjętą praktyką wykorzystywaną przez sprawców w międzyczasie jest zachęcenie inwestującego do odbycia rozmowy z analitykiem, do którego następnie zostaje połączony. Ten przedstawia mu zazwyczaj w *stricte* specjalistycznym języku rynek i giełdę kryptowalut, podkreślając jego atrakcyjność i bezpieczny charakter. Okoliczność ta – podobnie

[274] C. Bhardwaj, *Blockchain vs DLT – An Explanatory Guide You Can't Miss On,* https://appinventiv.com/blog/blockchain-vs-dlt-guide/ (dostęp: 20.06.2023 r.)
[275] Szerzej: A. Behan, *Waluty wirtualne jako przedmiot przestępstwa,* Krakowski Instytut Prawa Karnego Fundacja, Kraków 2022, s. 165 i nast.

jak wyżej opisywane – wzmacnia poczucie zaufania do doradców oraz platformy obsługującej pokrzywdzonego[276]. Kolejno, po przekazaniu kolejnych środków finansowych, doradca informuje, iż inwestycja się udała, wskaźniki giełdowe obrały pozytywny dla inwestującego kierunek, a zarobione pieniądze przybrały nieprawdopodobne dla inwestującego wartości. Kolejny etap, w celu wyłudzenia kolejnych pieniędzy, polega na tym, iż sprawca wskazuje, że celem zweryfikowania autentyczności numeru rachunku bankowego podanego jako właściwy dla wypłaty zysku, koniecznie jest wykonanie przelewu na optymalnie niewysoką sumę pieniędzy, co pokrzywdzony – mający wizję uzyskania niebotycznych zarobków oraz poniekąd zmiany w ten sposób swojego dotychczasowego życia – czyni niemalże niezwłocznie. Właśnie teraz nadchodzi krytyczny dla inwestującego moment, w którym kontakt ze sprawcą się urywa. Dotychczas bezproblemowo funkcjonujące numery telefonów, przestają być aktywne. Strona internetowa nie działa lub też nie jest przydatna dla nawiązania kontaktu. Złożenie reklamacji do banku i wstrzymanie uprzednio zleconych transakcji na olbrzymie kwoty jest już niemożliwe. Po bezskutecznym wykonaniu kilku czy też kilkunastu połączeń do pośrednika w inwestowaniu kryptowalut, pokrzywdzony zdaje sobie sprawę, iż został ofiarą przestępstwa oszustwa.

Analiza oraz ocena prawnokarna omawianego cyberprzestępstwa jest kolejnym przypadkiem w sposób w zasadzie jednoznaczny potwierdzającym założoną na wstępie niniejszego rozdziału tezę, zgodnie z którą cyberprzestępstwa w zdecydowanej większości przypadków przybierają postać podstawowego typu przestępstwa oszustwa. Sposób działania sprawcy w przypadku oszustwa „na bitcoina" w sposób ewidentny wypełnia znamiona przestępstwa spenalizowanego w art. 286 § 1 k.k., które wyczerpująco zostały omówione przy okazji omawiania pierwszych typów cyberprzestępstw i które w tej wersji przedstawiają się niemal identycznie, z tym zastrzeżeniem, iż sprawca wprowadza pokrzywdzonego w błąd co do możliwości szybkiego zainwestowania i zarobienia pieniędzy składając zapewnienie co do niemalże stuprocentowej szansy na pomyślny przebieg inwestycji.

1.3. Nowe technologie jako domena cyberprzestępców

Całokształt wyżej opisanych faktów dotyczących *stricte* sposobu działania cyberprzestępców wyraźnie wskazuje, iż nowe technologie w sposób bezpośredni wpływają nie tylko na statystykę dotyczącą przestępstw popełnionych przy wykorzystaniu sieci

[276] Szerzej o socjotechnikach: J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Uniwersytet w Białymstoku, Białystok 2017

teleinformatycznej w szerokim ujęciu, ale również determinują sposób działania sprawców. Im nowsze technologie pojawiają się na rynku, tym bardziej złożony i skomplikowany, a w konsekwencji trudny do wykrycia jest sposób działania sprawców, którzy te technologie wykorzystują dla celów przestępczych. Przy okazji omawiania konkretnych typów cyberprzestępstw skonkretyzowano precyzyjnie jakie środki komunikacji elektronicznej lub instrumenty wykorzystujące nowe technologie są w zasięgu działania sprawców. Metody te bezpośrednio zestawić należy z algorytmem działania organów ścigania, dla których środki te są punktem wyjścia dla pozyskania kolejnych danych a w konsekwencji, co najistotniejsze, dla wykrycia i ustalenia tożsamości sprawcy lub sprawców cyberprzestępstw.

Na tle niniejszej pracy wielokrotnie już podkreślano, iż postęp technologiczny jest na tyle dynamiczny, iż niemalże niemożliwe jest zapewnienie maksymalnego bezpieczeństwa i ochrony dla użytkowników nowych technologii oraz stworzenie takiego zaplecza prawnego, które w pełni odpowiadałoby temu postępowi. Sprawcy cyberprzestępstw posiadają natomiast dostęp do takich instrumentów i środków, które pośrednio zapewniają im anonimowość lub co najmniej w sposób znaczny utrudniają (lub uniemożliwiają) organom ścigania dotarcie do nich[277]. Jest to zdecydowanie kolejny aspekt wskazujący na negatywny wpływ rozwoju technologicznego na cyberbezpieczeństwo. Sprawcy nastawieni instrumentalnie na osiągnięcie konkretnego celu w postaci popełnienia czynu zabronionego i osiągniecia korzyści majątkowej wykorzystują szerokie spectrum technik[278], które bardzo często doprowadzają do „zmylenia" organów ścigania, które na podstawie konkretnych danych okazuje się, iż zmierzają w zupełnie przeciwnym kierunku aniżeli faktyczne wykrycie sprawcy, mimo iż konkretne okoliczności mogłyby wskazywać odmiennie.

Udostępnienie przez instytucje bankowe możliwości utworzenia rachunku bankowego za pośrednictwem sieci teleinformatycznej, w zasadzie poprzez wypełnienie niezbyt skomplikowanego formularza, na podstawie którego zawierana jest umowa o rachunek bankowy i generowany jest konkretny numer, otworzyło cyberprzestępcom możliwość tworzenia kont bankowych na tzw. „słupów"[279]. Proceder sprowadza się do tego, iż za udzielenie niewielkiej korzyści majątkowej, przypadkowa osoba osobiście w placówce banku lub w zdecydowanej większości przypadków przez Internet zakłada rachunek bankowy na

[277] Szerzej: K. Dziedzic, *Jak skutecznie zapewnić sobie anonimowość. Anonimowość w Internecie. Kompletny poradnik krok po kroku, „Komputer i Świat"*, 2018 nr 1

[278] Szerzej: O. Hostettler, *Darknet, Die Schattenwelt des Internets*, Zurych 2017

[279] Przykład oszustwa w roli słupa, por. Wyrok Sądu Apelacyjnego w Poznaniu z dnia 12 lipca 2022 roku sygn. II AKa 55/21, LEX nr 3441059

swoje dane, udostępniając go następnie sprawcom[280]. W ten sposób mają oni dostęp do konta, za pośrednictwem którego mogą przyjmować oraz przetransferować wyłudzone środki finansowe, a organy ścigania zostaną doprowadzone do osoby, która w rzeczywistości nie dopuściła się przestępstwa, a jedynie posłużono się jej danymi. Oczywiście analizie prawnokarnej można byłoby również poddać tą czynność sprawczą, chociażby w aspekcie pomocnictwa[281], niemniej jednak nie ma to *stricte* znaczenia dla rzeczonej tematyki. Analogicznie kwestia ta przedstawia się w przypadku rejestracji kart SIM, o czym wspominano przy okazji podkreślania pewnego rodzaju wady i bezsensowności wprowadzenia obowiązku rejestracji kart SIM i systemu tą rejestrację obsługującego. W tym przypadku sprawcy mogą zarejestrować numer telefonu na nie tylko dowolną osobę, ale również na fikcyjne dane. Ponownie pozyskane przez prowadzącego dane telekomunikacyjne nie doprowadzą do wykrycia sprawcy, jak również nie naprowadzą do miejsca jego rzeczywistego działania.

Oprócz wyżej wymienionych metod, w odniesieniu do których celowe byłoby przypisanie im przymiotu podstawowych, sprawcy wykorzystują również bardzo złożone, skomplikowane i specjalistyczne techniki bezpośrednio związane z funkcjonowaniem nowych technologii. Jako pierwszą kategorię wskazać należy techniki maskujące ruch w sieci. Jedną z najbardziej popularnych technik w tym zakresie jest tzw. technika TOR, wykorzystywana nie tylko przez cyberprzestępców na terenie kraju, która również słynie szeroko wykorzystywany i bardzo popularny instrument na całym świecie, który najbardziej zyskał na popularności w XXI wieku, z uwagi na dynamiczny wzrost cyberprzestępstw. TOR jest to internetowa sieć, która uznawana jest za najbardziej bezpieczną możliwość zachowania anonimowości przy korzystaniu z Internetu[282].

Najbardziej popularną przeglądarką w tym zakresie jest „Tor Browser"[283], ale istnieje również wiele innych przeglądarek. Przyjmuje się, iż w przypadku działania TOR[284] za pomocą kryptografii, wielowarstwowo szyfrowane są wszelkie pakiety danych przesyłane przez różne serwery, które nie rozpoznają danych, które w rzeczywistości przesyłają[285]. Aby zobrazować

[280] Por. wyrok Sądu Okręgowego w Siedlcach z dnia 18 maja 2022 roku, sygn.. II Ka 198/22, LEX nr 3353329
[281] Por. Okoliczności świadczące o pomocnictwo w formie „słupa" w oszustwie, por. Wyrok Sądu Apelacyjnego w Gdańsku z dnia 16 marca 2022 r. sygn.. II AKa 263/21, LEX nr 3359776
[282] J. Bell, B. Schneier, G. Greenwald, *NSA and GCHQ target* Tor *network that protects anonymity of web users,* www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption, dostęp: 10.06.2023 r.
[283] C. Zielińska *„Cybercrime" – wzywanie dla kryminologii* [w:] D. Dajnowicz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E.W. Pływaczewski (red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku*, 2022, s. 541
[284] *The Onion Router*
[285] K. Dziedzic, *Jak skutecznie zapewnić sobie anonimowość. Anonimowość w Internecie. Kompletny poradnik krok po kroku, „Komputer i Świat"*, 2018 nr 1, s. 6

ten zabieg, wskazać należy, iż w normalnych, typowych warunkach korzystania z Internetu, bez użycia sieci TOR, wpis konkretnego adresu w przeglądarkę powoduje, że żądanie dostępu do pewnej strony internetowej ujawnia odpowiedniemu operatorowi sieci telekomunikacyjnej adres IP, z którego dane żądanie zostało wysłane, umożliwiając w ten sposób – jak wyżej wskazano – organom ścigania zidentyfikowanie sprawcy przestępstwa. Wpisanie adresu w przeglądarkę powoduje nie tylko ujawnienie adresu IP, z którego wyszło żądanie, ale również adresu IP docelowego, czyli tego, do którego sygnał dotarł. Zatem wykorzystanie techniki TOR w pewien sposób maskuje – w skrócie ujmując – adres IP użytkownika i przesyłane żądanie dostępu do danej witryny internetowej[286]. Trasa przesyłanych danych przebiega wówczas przez różnego rodzaju węzły, powodując w ten sposób, iż adres IP użytkownika pozostaje ukryty, co uniemożliwia dostawcy Internetu odszyfrowanie adresu IP[287].

1.4.Identyfikacja cyberprzestępców

Sposób działania i funkcjonowania organów ścigania musi być zorganizowany we właściwy sposób, aby zapewnić i umożliwić maksymalną realizację nałożonych na nich zadań, to jest przede wszystkim dążyć do wykrycia przestępstw oraz ściągania ich sprawców[288]. Nie ma wątpliwości co do tego, iż metody te muszą być nieustannie i sukcesywnie udoskonalane, modernizowane tak, aby w sposób możliwie najbardziej pełny wykorzystać ich potencjał. Zespoły prokuratorów, ale również specjalistów z wielu dziedzin, w tym również pozaprawnych poświęcają mnóstwo czasu, aby opracować pewne szablony i schematy działania, które konsekwentnie będą prowadzić do wykrywania sprawców przestępstw i pociągania ich do odpowiedzialności karnej.

Jednoznacznie podkreślić należy, iż absolutnie nie ma możliwości stworzenia jednakowego algorytmu działania dla wszystkich przestępstw. Katalog czynów zabronionych przewidzianych zwłaszcza w kodeksie karnym, ale również w szeregu innych aktów prawnych, w których przewidziane są dyspozycje karne, w tym w szczegółowych ustawach, np. ustawie Prawo ochrony środowiska[289], ustawie o ochronie zwierząt[290] czy też ustawie

[286] J. Bell, B. Schneier, Greenwald G., *NSA and GCHQ target* Tor *network that protects anonymity of web users*, www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (dostęp: 10.06.2023 r.)
[287] O. Hostettler, *Darknet, Die Schattenwelt des Internets*, Zurych 2017, s. 30
[288] M. Kurowski [w:] D. Świecki (red.), *Kodeks postępowania karnego. Tom I. Komentarz*, Wolters Kluwer, Warszawa, 2023
[289] Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz. U. z 2022 r. poz. 2556 ze zm.)
[290] Ustawa z dnia 21 sierpnia 1997 r. o ochronie zwierząt (Dz. U. z 2022 r. poz. 572, 2375)

o przeciwdziałaniu narkomanii[291] lub ustawie o rachunkowości[292], jest bardzo szerokim zagadnieniem, w związku z czym w pełni zrozumiałe jest to, że brak jest możliwości stworzenia uniwersalnego schematu działania dla organów ścigania, który sprawdziłby się w każdym przypadku. Każde przestępstwo narusza inne dobra prawnie chronione, popełnione zostać może przez inny podmiot, dotyczy innej czynności sprawczej i popełnione może zostać przy wykorzystaniu różnych instrumentów. Zatem metodyka organów ścigania powinna zostać dopracowana w sposób w pełni odpowiadający specyfice danego czynu zabronionego.

Podkreślenia wymaga jednak kategorycznie fakt, iż żaden, chociażby najbardziej skrupulatnie opracowany algorytm działania organów ścigania, nawet przygotowany przez przodujących specjalistów nie będzie idealną kalką dla przestępstw, dla których został przygotowany, albowiem nie ma dwóch takich samych przestępstw i dwóch takich samych ich sprawców. Każdorazowo dostrzec można pewne znaczące różnice w sposobie realizowania znamion czynu zabronionego. W związku z powyższym, organy prowadzące postępowania przygotowawcze, mają pełną świadomość konieczności regularnego dopracowywania i precyzowania przyjętego algorytmu działania w odniesieniu do konkretnej nadzorowanej i prowadzonej sprawy. Wyłącznie taki model działania zapewni prawidłowy tok postępowania, które wówczas przebiegało będzie wedle konkretnie przyjętych etapów, pozwalający w konsekwencji zakończenie postępowania przygotowawczego sporządzeniem decyzji merytorycznej poprzez skierowanie aktu oskarżenia do właściwego miejscowo i rzeczowo sądu. Niemniej jednak nie ma wątpliwości co do przydatności i konieczności opracowywania oraz regularnego dopracowywania algorytmów działania organów ścigania. Są one skrupulatnie przygotowywane przez specjalistów, którzy podejmują m.in. próby nadążenia nad postępem technologicznym oraz sposobami działania sprawców, dążąc do tego, aby wszelkie schematy wykrywania przestępstw i ścigania sprawców były możliwie najbardziej aktualne. Wówczas w sposób zdecydowany usprawniony zostaje sposób funkcjonowania m.in. prokuratorów i innych organów prowadzących postępowanie przygotowawcze, co z kolei pozwala na szybsze wykrycie sprawców przestępstw, a podkreślić należy wyraźnie, iż zazwyczaj czas ma kluczowe znaczenie i bywa „nieprzyjacielem" organów ścigania. Nadto dzięki odpowiednio opracowanym algorytmom sposób procedowania organów pomimo działalności w różnych jednostkach na terenie całego kraju, jest niejako „zuniwersalizowany".

[291] Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz.U. z 2023 r. poz. 172)
[292] Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2023 r. poz. 120, 295)

Na kanwie przedmiotowych rozważań, z uwagi na specyfikę badań oraz ich analizy, podjęta zostanie próba możliwie najbardziej precyzyjnego i dogłębnego przeanalizowania algorytmów działania organów ścigania w odniesieniu do cyberprzestępstw jako takich ogólnie oraz w odniesieniu do konkretnych ich rodzajów, omówionych w poprzednim rozdziale. Nadto, po uprzednio przeprowadzonej analizie, możliwa będzie ocena ich skuteczności oraz zupełności, a także opisanie wniosków w tym zakresie, ewentualnie wyrażenie pewnych postulatów, które mogłyby udoskonalić te schematy i usprawnić postępowania przygotowawcze oraz sposób działania organów ścigania.

W pierwszej kolejności podkreślić należy, zdaje się oczywisty fakt, iż zwalczanie cyberprzestępczości stanowi dla organów ścigania tak samo istotne zadanie jak zwalczanie każdej innej przestępczości, z tą przeciwko życiu i zdrowiu na czele. Niemniej jednak z uwagi na bardzo charakterystyczny sposób działania sprawców i zastosowanie innego medium popełnienia czynu zabronionego, bo z wykorzystaniem szeroko rozumianej sieci teleinformatycznej i cyberprzestrzeni, organy ścigania zmuszone są do stosowania odmiennych metod aniżeli w przypadku przestępczości tzw. pospolitej[293]. Jak wyżej wielokrotnie wskazywano proces wykrywczy musi się odbyć w ściśle określonym czasie[294]. W związku z tym, iż cyberprzestępstwa popełniane są przy wykorzystaniu nowych technologii, za pośrednictwem tzw. wirtualnego świata, wszelkich śladów mogących przyczynić się do identyfikacji cyberprzestępców należy poszukiwać również w wirtualnym świecie. Biorąc pod uwagę rzeczoną okoliczność ślady takie nazwać należy śladami wirtualnymi.

2. Etapy procesu wykrywczego

W praktyce przyjmuje się pewne ogólne metody działania organów ścigania, mające zastosowanie w przypadku procesu wykrywczego wszystkich typów cyberprzestępstw, które niemniej jednak należy dostosowywać do konkretnej sprawy[295]. Z uwagi na nieustannie rosnącą popularność chociażby oszustwa metodą „na bitcoina" w tej sferze wypracowano odrębny algorytm działania organów ścigania, co nie oznacza, iż przywołane na wstępie ogólne metody działania dotyczące cyberprzestępstw nie znajdą w tym przypadku zastosowania. W związku z tym przyjmuje się, iż w celu zidentyfikowania sprawcy cyberprzestępstwa niezbędne jest

[293] R. Jedlińska, *Problem przestępczości elektronicznej*, „Elektroniczne Problemy Usług" 2017/1, s. 191 i nast.
[294] Ł. Krysiński, *Identyfikacja cyberprzestępców,* Prok. I Pr. 2020/2/120-134
[295] Szerzej: D. Taberski, *Postępowania w sprawach o oszustwa popełnione za pośrednictwem Internetu,* Prokuratura i Prawo 2018/6/63-83

wykonanie wielu czynności, w tym procesowe zabezpieczenie danych, które można podzielić na pięć etapów:

1. zgromadzenie pełnych danych dotyczących cyberzdarzenia;
2. opisanie cybersprawcy za pomocą wykorzystanych przez niego danych wirtualnych;
3. ustalenie danych użytkownika korzystającego z usług świadczonych drogą elektroniczną u administratora lub operatora sieci telekomunikacyjnych;
4. dokonanie reasumpcji materiału dowodowego;
5. wykonanie czynności procesowych z osobowymi środkami dowodowymi.

W związku z wyróżnieniem pięciu podstawowych etapów, które z założenia mają doprowadzić organy ścigania do pociągnięcia sprawców cyberprzestępstw do odpowiedzialności karnej i które mają niejako charakter uniwersalny, ewentualnie modyfikowany przy konkretnych typach cyberprzestępstw, priorytetowo należy potraktować ich szczegółowe omówienie na tle niniejszej pracy.

2.1. Zgromadzenie informacji dotyczących popełnienia cyberprzestępstwa

Pierwszy, najczęściej kluczowy z punktu widzenia ustalenia tożsamości sprawcy etap algorytmu działania organów ścigania odnosi się do precyzyjnego i możliwie najbardziej dokładnego ustalenia stanu faktycznego. Oczywiście powzięcie przez organy ścigania informacji o przestępstwie popełnionym przy wykorzystaniu nowych technologii, jest pierwszym momentem inicjującym podjęcie jakichkolwiek czynności procesowych zmierzających do ustalenia sprawcy przestępstwa. Bez formalnego zawiadomienia o popełnieniu przestępstwa co do zasady brak jest przesłanek zarówno faktycznych jak i prawnych do rozpoczęcia procesu wykrywczego. Jedynie zasygnalizować należy, iż w zdecydowanej większości postępowania przygotowawcze, których przedmiotem są cyberprzestępstwa, inicjowane są na skutek zawiadomienia o przestępstwie złożonego przez pokrzywdzonego czynem zabronionym, ewentualnie przez instytucje, których działalność została wykorzystana dla celów przestępczych, np. banki. Niemniej jednak zdarzają się również sprawy, które zostają wszczynane na skutek czynności operacyjnych przeprowadzanych przez organy ścigania, np. wydziały do walki z cyberprzestępczością organizowane najczęściej przy komendach wojewódzkich policji.

Zebranie informacji dotyczących zdarzenia nie bez powodu uznawane jest za najważniejszy etap procesu wykrywania sprawcy lub sprawców, albowiem czynność ta bezpośrednio determinuje możliwość procesowego zabezpieczenia wirtualnych śladów, które

są kluczowe w przypadku wykrywania cyberprzestępstw[296]. To ile faktów i danych ustalimy na tym etapie wpłynie na rzeczywistą możliwość ustalenia i zidentyfikowania sprawcy cyberprzestępstwa, dlatego niezwykle istotne jest rzetelne i właściwe przyjęcie do protokołu ustnego zawiadomienia o popełnieniu przestępstwa oraz przesłuchanie pokrzywdzonego[297]. Odpowiednie sformułowanie pytań podczas przesłuchania jest kluczowe, albowiem w swobodnej wypowiedzi pokrzywdzony, będąc pod wpływem silnych emocji jako ofiara socjotechnik stosowanych przez sprawcę, może pominąć, w tym również nieświadomie pewne istotne elementy. Biorąc to pod uwagę, wykonanie tych czynności przez doświadczonego funkcjonariusza w sposób zdecydowany wpłynie na prawidłowy tok postępowania przygotowawczego jak również na przebieg pozostałych etapów procesu wykrywczego.

Zgromadzenie danych dotyczących zdarzenia, a pośrednio również sprawcy, jak już wyżej wspominano, rozpoczyna się od ustalenia dokładnego czasu, w którym doszło do popełnienia czynu zabronionego. Kolejno, co jest równie istotne, należy zebrać pełne informacje dotyczące określenia sposobu komunikacji ze sprawcą (np. portal sprzedażowy, portal społecznościowy, komunikator społecznościowy, aplikacja mobilna). Ustalenie medium, za pomocą którego komunikowano się z pokrzywdzonym w przypadku cyberprzestępstw jest bardzo istotne, albowiem już u źródła, najczęściej administratora danej domeny organy ścigania są w stanie otrzymać kolejne wirtualne ślady o sprawcy[298]. Kolejnym etapem jest uzyskanie pełnych informacji dotyczących sprawcy, nawet wówczas kiedy wydaje się, iż w toku przestępczego procederu wykorzystał techniki maskujące ruch w sieci lub inne instrumenty mające na celu zmylenie organów ściągania, albowiem nawet pozornie nieprzydatne dane, w powiązaniu z konkretnymi ustaleniami mogą okazać się przydatne w procesie wykrywczym. Wśród danych identyfikujących sprawcę ustalić z pewnością należy m.in. nazwę użytkownika na portalu społecznościowym oraz ewentualnie numer ogłoszenia, które wykorzystano dla celów przestępczych, wszelkie numery kontaktowe oraz adresy poczty elektronicznej, którymi się posługiwał sprawca. Nadto istotne jest ustalenie sposobu przekazania sprawcy pieniędzy, w tym ustalenie numeru rachunku bankowego, na rzecz którego dokonano transferu środków finansowych, ewentualnie numeru telefonu, który został przypisany do metody płatności BLIK. Konkludując, zebranie informacji dotyczących zdarzenia dotyczy przede wszystkim ustalenia

[296]Szerzej: A. Machnacz., *Gromadzenie i zabezpieczanie materiału dowodowego w zakresie przestępstw komputerowych* [w:] red. J. Kosiński, *Przestępczość teleinformatyczna*, 2014

[297] D. Taberski, *Postępowania w sprawach o oszustwa popełnione za pośrednictwem Internetu,* Prokuratura i Prawo 2018/6/63-83

[298] Szerzej: M. Rogalski, *Udostępnianie danych telekomunikacyjnych sądom i prokuratorom*, Prokuratura i Prawo 2015, nr 12, s. 61 i nast.

wszelkich jego szczegółów, a zwłaszcza ustalenia nowych technologii, za pomocą których komunikowano się na odległość z pokrzywdzonym i przypisanych im konkretnych danych[299].

2.2. Opisanie cyberprzestępcy za pomocą wykorzystanych przez niego nowych technologii

Tak jak w przypadku przestępstw o charakterze powszechnym, sprawca realizując czynność sprawczą, co do zasady zawsze pozostawia pewne ślady, które następnie wykorzystywane są przez organy ścigania w celu jego zidentyfikowania, tak w przypadku cyberprzestępstw sprawcę można opisać poprzez nowe technologie, które zostały przez niego wykorzystane dla celów przestępczych oraz poprzez ślady, które działając w ten sposób zostawił.

Na jednym z pierwszych etapów algorytmu ścigania sprawców przestępstw w zasadzie brak jest możliwości jednoznacznego opisania sprawcy poprzez dane w pełni go identyfikujące, to jest poprzez jego dane osobowe[300]. Niemniej jednak nie oznacza to, iż brak jest jakiejkolwiek możliwości pewnego skonkretyzowania jego cech, które następnie na podstawie czynności procesowych realizowanych w kolejnych etapach, mogą doprowadzić do pełnego zidentyfikowania sprawcy przestępstwa oraz pociągnięcia do odpowiedzialności karnej. Sprawca cyberprzestępstwa może zostać opisany poprzez numer MSISDN, numer IP, numer (nazwa) użytkownika na portalu sprzedażowym, nazwa użytkownika na portalu społecznościowym, numer rachunku bankowego, lokalizacja bankomatu, z którego doszło do wypłacenia środków, konkretną aplikację wykorzystaną do komunikacji z pokrzywdzonym. Podkreślenia wymaga fakt, iż na podstawie poczynionych w ten sposób ustaleń, w tym dokładnego określenia stanu faktycznego, a następnie rzetelnego przyjęcia zawiadomienia o przestępstwie i na tej podstawie opisanie sprawcy przestępstwa za pomocą środków komunikacji elektronicznej, którymi się posłużył, możliwe będzie następnie procesowe zabezpieczenie danych, zwłaszcza danych retencyjnych oraz poszukiwanie użytkownika u podmiotu świadczącego usługi drogą elektroniczną[301].

---

[299] A. Wolska-Bagińska, *Metodyka prowadzenia postępowań w sprawach z wykorzystaniem domen internetowych* [w:] A. Krasuski, A. Wolska-Bagińska, O. Zienkiewicz-Będźmirowska, *Działania naruszające prawa do domen internetowych*, Wolters Kluwer, 2021, s. 163 i nast.

[300] Szerzej: G. Martyniak, A. Wojciechowski, *Metodyka czynności w sprawach przestępstw popełnianych z wykorzystaniem sieci Internet*, (w:) J. Kosiński, S. Kmiotek (red.), *Przestępczość Teleinformatyczna*, 2011

[301] Szerzej: M. Rogalski, *Udostępnianie danych telekomunikacyjnych sądom i prokuratorom*, Prokuratura i Prawo 2015, nr 12, s. 61 i nast.

2.3. Procesowe pozyskanie danych retencyjnych

W związku z tym, iż dynamika rozwoju nowych technologii jest ogromna, a w konsekwencji odnotowany wzrost liczby cyberprzestępstw popełnionych w ostatnich latach[302], ustawodawca musi niejako nadążać nad rzeczonymi zmianami wprowadzając do obrotu prawnego takie instrumenty, które zapewnią bezpieczeństwo w sieci, a w przypadku jego naruszenia pozwolą na dotarcie do sprawcy przestępstwa. Dziedzina kryminologii jest bardzo obszerna i przewiduje liczne metody i techniki działania organów ścigania, które pozwalają na zidentyfikowanie sprawców przestępstw. Niemniej jednak z uwagi na stosunkowo nowy rodzaj przestępstwa oraz nieustannie ulepszane i modernizowane techniki działania cybersprawców, metody działania organów ścigania również muszą być w ten sposób udoskonalane. Na tle niniejszej części rozważań analizie poddane zostaną środki i instrumenty, którymi dysponują organy ścigania, które to środki mają na celu poszukiwanie i zidentyfikowanie sprawcy przestępstwa, a także możliwości i sposoby ich wykorzystania.

Kilkukrotnie wyżej wskazywano, iż w pierwszym etapie procesu wykrywczego, niezbędne jest precyzyjne ustalenie czasu, w którym sprawca działał. Okoliczność ta jest kluczowa z punktu widzenia wielu kwestii, niemniej jednak w tym miejscu w pełni celowe i uzasadnione jest przeanalizowanie kwestii retencji danych[303]. Dane retencyjne to zazwyczaj dane telekomunikacyjne w postaci historii połączeń, logowań do stacji BTS, historii rozmów, wykazu logowań do kont użytkowników na różnych platformach, które są przechowywane przez właściwych operatorów sieci komórkowych oraz administratorów domen internetowych przez ściśle określony czas, po upływie którego zostają usuwane z baz danych i nie ma możliwości ich ponownego odtworzenia. W zależności od porządku prawnego, który jest obowiązujący na terytorium danego kraju, okres przechowywania – retencji jest inny[304]. W związku z tym, iż tłem przedmiotowych rozważań jest prawo powszechnie obowiązujące w Polsce, wskazać należy, iż co do zasady okres retencji danych wynosi rok[305]. Po upływie tego czasu, zwracanie się o dane telekomunikacyjne przez organy ścigania jest w zasadzie

[302]https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63976,Oszustwo-art-286.html, (dostęp: 05.05.2023 r.)

[303] M. Kiziński, *Retencja danych telekomunikacyjnych,* Prokuratura i Prawo 2016/1/138-155

[304] Szerzej o retencji danych w różnych porządkach prawnych: J. Kudła, Retencja danych a prawo UE. Omówienie wyroków TS z dnia 20 września 2022 r., C-793/19 i C-794/19 (SpaceNet i in.) oraz C-339/20 i C-397/20 (VD i SR), 2022 oraz M. Rojszczak, *Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna,* Państwo i Prawo 2023/2/33-58

[305] Art. 180a ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, szerzej: A. Krasuski, *Prawo telekomunikacyjne. Komentarz.,* wyd. IV, 2015

bezcelowe, albowiem szanse na uzyskanie jakichkolwiek informacji umożliwiających identyfikację sprawcy są niewielkie[306]. Etap procesu wykrywczego dotyczący procesu pozyskiwania konkretnych danych umożliwiających identyfikację sprawcy cyberprzestępstwa na podstawie informacji uzyskanych od szeroko rozumianych operatorów telekomunikacyjnych uznawany jest za najtrudniejszy i najbardziej złożony. Proces ten oceniany w praktyce jest jako najbardziej długotrwały, co spowodowane jest procedurą związaną z pozyskaniem tych danych, która poddana zostanie szczegółowej analizie w dalszej części rozważań. Na długotrwałość rzeczonego procesu bezpośrednio wpływa również czas uzyskiwania odpowiedzi od administratorów, a niejednokrotnie także potrzeba zwrócenia się o kolejne dane retencyjne na ich podstawie.

Po opisaniu sprawcy cyberprzestępstwa za pomocą tzw. śladów o charakterze wirtualnym, które zostały pozostawione przez niego w toku przestępczego procederu, w celu ustalenia tożsamości sprawcy przestępca, w kolejnym etapie procesu wykrywczego, należy ustalić administratora lub ewentualnie inny podmiot, który świadczy usługą drogą elektroniczną. W zależności od środka komunikacji, za pomocą którego zachodzi konieczność podjęcia czynności zmierzających do identyfikacji, będą to właściciele lub administratorzy stron internetowych, adresów stron internetowych czy też operatorzy sieci telekomunikacyjnych. Mając wiedzę na temat numeru ogłoszenia, numeru abonenta czy też adresu poczty elektronicznej wykorzystanej przez sprawcę otwiera się przez organami ścigania możliwość procesowego zabezpieczenia a następnie uzyskania danych, które chociażby w części przyczynią się do ustalenia jego tożsamości[307]. W tym celu w pierwszej kolejności należy przygotować swoistego rodzaju listę danych, które są w posiadaniu organów ścigania, o których wyczerpująco wspomniano w poprzedniej części rozważań. Następnie za pomocą ogólnodostępnych stron internetowych należy zweryfikować kto jest administratorem, operatorem czy też właścicielem odpowiednio adresu mailowego, numeru telefonu czy też strony internetowej. W celu ustalenia operatora sieci komórkowej, który obsługuje uprzednio ustalony numer telefonu, można skorzystać ze strony internetowej https://www.mgsm.pl/pl/wjakiejsieci. Po wpisaniu numeru telefonu, operator strony wskaże w jakiej sieci został zarejestrowany pierwotnie dany numer i ewentualnie do jakiej sieci następnie został przeniesiony. Za pomocą domeny https://www.whois.com istnieje możliwość ustalenia

[306] A. Krasuski, *Prawa i obowiązki abonentów usług telekomunikacyjnych*, 2021
[307] M. Rogalski, *Udostępnianie danych telekomunikacyjnych sądom i prokuratorom*, Prokuratura i Prawo 2015, nr 12, s. 61 i nast.

administratora domeny internetowej, za pomocą którego doszło do zarejestrowania domeny, czy też administratora adresu poczty elektronicznej, który gromadzi i przechowuje dane dotyczące użytkownika skrytki pocztowej elektronicznej. Nadto przewidziano możliwość ustalenia operatora sieci komórkowej, w tym internetowej właściwego dla uprzednio ustalonego użytkownika IP. Weryfikację w tym zakresie również można przeprowadzić za pośrednictwem ogólnodostępnej strony internetowej https://www.ripe.net, w formularz której wystarczy wpisać wyłącznie uprzednio ustalony adres IP, bez konieczności wskazywania dokładnego czasu w sieci, w którym sprawca działał. Mając wiedzę na temat konkretnych danych, które na potrzeby niniejszych rozważań można nazwać „numerycznymi", ale również o właściwych operatorach „obsługujących" te dane, można podjąć próby zmierzające do procesowego zabezpieczenia oraz poszukiwania danych użytkownika u podmiotu świadczącego usługi drogą elektroniczną.

Z praktycznego i procesowego punktu widzenia dla wykonania rzeczonej czynności niezbędne jest sporządzenie postanowienia o żądaniu wydania rzeczy[308] zaadresowanego do ustalonego uprzednio operatora lub administratora. Zaznaczyć jednak wyraźnie należy, iż czynność ta figuruje jako zastrzeżona wyłącznie dla działalności prokuratora, natomiast brak jest procesowej możliwości zabezpieczenia i pozyskania danych przez inne organy prowadzące postępowania przygotowawczego, w tym Policję, z tym jednak zastrzeżeniem, iż jest to możliwe wyłącznie w przypadku tzw. czynności operacyjnych, np. na podstawie at. 20c ust. 1 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Policji[309]. Zaznaczyć należy również, iż brak jest jakichkolwiek podstaw prawnych zezwalających prokuratorowi na zlecenie czy powierzenie wykonania tej czynności procesowej w ramach prowadzonego postępowania[310]. Nadto wskazać należy, iż dopiero na etapie prowadzonego postępowania przygotowawczego ustawodawca dopuszcza możliwość uzyskania danych telekomunikacyjnych, co oznacza, iż wykonanie tej czynności procesowej, nie jest możliwe na etapie postępowania sprawdzającego, a dopiero po wszczęciu postępowania przygotowawczego w formie odpowiednio dochodzenia lub śledztwa.

Zanim analizie poddane zostaną przepisy postępowania karnego oraz tzw. przepisy szczegółowe, będące podstawą do skutecznego i legalnego procesowego uzyskania danych telekomunikacyjnych i danych retencyjnych, przeanalizować należy w pierwszej kolejności katalog danych, co do których istnieje w ogóle możliwość ich pozyskania. Kwestia ta została

[308] W trybie 180 § 1, 218 § 1 i 2 k.p.k. oraz art. 179 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne
[309] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2023 r. poz. 171)
[310] R. Stefański (red.), S. Zabłocki (red.), *Kodeks Postępowania Karnego. Tom III. Komentarz do art. 297-424,* 2021

uregulowana m.in. w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[311], w której ustawodawca określił precyzyjnie jakie informacje może przetwarzać usługodawca w związku ze świadczeniem usług, a są to w szczególności: nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL, ewentualnie numer paszportu, dowody osobistego lub innego dokumentu weryfikującego tożsamość, adres zameldowania na pobyt stały lub adres do korespondencji, jeśli jest inny, dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy poczty elektronicznej usługobiorcy, dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia, w tym m.in. numer rachunku bankowego, ewentualnie – za zgodą usługobiorcy i dla szeroko rozumianych celów marketingowych – inne dane usługobiorcy, które nie są niezbędne dla świadczenia usługi drogą elektroniczną. Jak wskazano, katalog informacji dotyczących usługobiorcy, a zatem z punktu widzenia omawiania rzeczonej materii również dotyczących sprawcy, jest bardzo szeroki a szansa ustalenia tożsamości sprawcy oraz jego identyfikacji lub ewentualnego pozyskania kolejnych danych umożliwiających tą identyfikację jest duża. Niemniej jednak podkreślić należy, iż wyżej wymieniony katalog informacji może być przetwarzany przez usługodawcę, tj. operatora lub administratora, może je gromadzić i przechowywać, aczkolwiek nie musi tego robić. Rzeczona ustawa w żaden sposób nie nakłada niestety na usługodawców obowiązku gromadzenia i przechowywania żadnych danych dotyczących ich usługobiorców.

Podając analizie środek, za pomocą którego prokurator ma możliwość pozyskania wyżej wspomnianych danych, zanim zbadana zostanie jego treść, precyzyjnie omówić należy podstawy prawne umożliwiające uzyskanie rzeczonych informacji. Zgodnie z postanowieniami art. 18 ust. 6 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną dane, które przechowuje, gromadzi i przetwarza usługodawca mogą zostać udostępnione w sposób nieodpłatny uprawnionym organom państwa na potrzeby prowadzonych przez nie postępowań. Udostępnianie tych danych odbywa się na podstawie odrębnych przepisów. W tym zakresie w pierwszej kolejności wskazać należy na przepisy postępowania karnego, zwłaszcza art. 180 § 1, art. 218 § 1 i 2 k.p.k., które w swojej treści bezpośrednio regulują kwestie możliwości zwolnienia z zachowania tajemnicy, w tym zawodowej i służbowej[312]. Ten zabieg jest niezbędny z punktu widzenia procesowego zabezpieczenia i pozyskania danych

[311] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
[312] Szerzej: K. Dudka (red.), *Kodeks postępowania karnego. Komentarz,* wyd. II, 2020, Szerzej na temat ochrony tajemnicy korespondencji na gruncie poszczególnych gałęzi prawa: A. *Gryszczyńska*, *Tajemnica korespondencji*, M. Praw. 2015/24, s. 1335 i n.

telekomunikacyjnych umożliwiających identyfikację sprawcy cyberprzestępstwa. W analizowanych przepisach również potwierdzany jest wymóg co do formy takiej decyzji procesowej, albowiem z treści art. 180 § 1 k.p.k. wynika, iż zwolnienie z tajemnicy odbywa się w formie postanowienia, na które przysługuje zażalenie. Zatem w zakresie formy w/w decyzji procesowej, zasygnalizować jedynie należy, iż każdorazowo musi mieć postać postanowienia. Wyłącznie taka forma zapewnia skuteczne pozyskanie właściwych danych w odpowiednim czasie.

Z kolei art. 218 § 1 k.p.k. niejako nakłada na operatorów sieci telekomunikacyjnej oraz administratorów domen internetowych, ewentualnie na innych usługodawców obowiązek udostępnienia danych objętych zakresem żądania danych wskazanych w postanowieniu. Ważną kwestią, bezpośrednio wpływającą na prawidłowy tok postępowania, jest treść § 2 wyżej wspomnianego przepisu, który umożliwia organom procesowym odroczenie doręczenia rzeczonego postanowienia o żądaniu wydania rzeczy abonentowi telefonu lub nadawcy, którego wykaz połączeń lub innych przekazów informacji został wydany, na czas oznaczony, lecz nie później niż do czasu prawomocnego zakończenia przedmiotowego postępowania. Obowiązek udostępnienia danych telekomunikacyjnych dodatkowo precyzuje znajdujący się w podstawie prawnej postanowienia o żądaniu wydania rzeczy art. 179 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[313]. Pomimo negatywnego aspektu wyżej wskazanych informacji dotyczących braku obowiązku przechowywania konkretnych danych, co mogłyby prowadzić do nieco błędnego przekonania, iż sytuacja ta pośrednio zamyka organom ścigania możliwość zabezpieczenia niezbędnych z punktu widzenia celów postępowania przygotowawczego danych, jednoznacznie wskazać należy, iż w praktyce sytuacja przedstawia się z pozytywnej strony i niebywale rzadko brak jest możliwości pozyskania tych danych. Omawiając kwestie praktyczne, przeanalizować należy jakie informacje spośród wyżej wskazanych są rzeczywiście gromadzone przez usługodawców i w jakim zakresie są one udostępniane organom ścigania w odniesieniu do konkretnych danych wymagających identyfikacji.

W zakresie najbardziej popularnych danych telekomunikacyjnych odnoszących się bezpośrednio do numeru abonenta wskazać należy, iż sporządzając postanowienie o żądaniu wydania rzeczy organ prowadzący postępowanie przygotowawcze, w tym przypadku prokurator najczęściej żąda udostępnienia następujących danych:

[313] M. Rogalski (red.), Prawo *telekomunikacyjne. Komentarz*. LEX 2010

- danych teleadresowych użytkownika numeru telefonu,
- wykazu połączeń przychodzących i wychodzących z konkretnego numeru telefonu w danym okresie (przy uwzględnieniu okresu retencji danych) wraz z wykazem stacji BTS, do których dane numery logowały się w tym okresie,

rzadziej również:

- danych abonentów występujących z połączeniach z użytkownikiem numeru telefonu,
- pełnych informacji dotyczących innych kart SIM współpracujących z danym numerem abonenta.

Co do zasady, przy zachowaniu okresu retencji danych, operator sieci komórkowej, przy założeniu, iż jest właściwy dla wskazanego numeru telefonu, udostępni na potrzeby postępowania przygotowawczego żądane dane telekomunikacyjne. Analogicznie kwestia ta przedstawia się w przypadku operatorów sieci komórkowych, lecz w przypadku, gdy żądanie dotyczy adresu IP. Wówczas organ prowadzący postępowanie przygotowawcze żąda od uprzednio ustalonego operatora danych osobowych użytkownika ustalonego numeru IP, przy dokładnym określeniu daty i godziny, z dokładnością co do sekundy czasu[314], w którym użytkownik działał w sieci, żądając również wskazania stacji BTS, za pośrednictwem której miało miejsce połączenie z Internetem, co umożliwi ustalenie ewentualnej lokalizacji użytkownika. Na skutek tego prokuratorowi na potrzeby postępowania karnego udostępniane są informacje co do dokładnych danych użytkownika numeru IP, ewentualnie precyzyjniej wskazany jest usługodawca sieci. W ten sposób możliwe jest wytypowanie osoby, na dane której zarejestrowano sieć Internetu. W odniesieniu do danych telekomunikacyjnych, które można procesowo zabezpieczyć na podstawie uprzednio ustalonego adresu poczty elektronicznej oraz administratora go obsługującego, poza danymi teleadresowymi i numerem telefonu, ustalić również można tzw. „zastępczy" adres mailowy, adres IP pierwszego i ostatniego logowania, jak również numery IP, które wykorzystano do logowania w okresie objętym żądaniem.

W związku z cyberprzestępstwami popełnianymi na bardzo szeroką skalę przy wykorzystaniu platform sprzedażowych oraz portali społecznościowych, zbiorczo wskazać należy jakie dane udostępniane są przez administratorów takich witryn i domen prowadzonych za pośrednictwem sieci teleinformatycznej. Jak się w praktyce okazuje, za pomocą tych danych, zachodzi duże prawdopodobieństwo ustalenia właściwych danych użytkownika końcowego, co

[314] W formacie gg:mm:ss

z kolei pozwala na ustalenie tożsamości sprawcy przestępstwa. Na skutek odpowiednio sporządzonego postanowienia o żądaniu wydania rzeczy oraz zwolnieniu z tajemnicy zawodowej, platformy sprzedażowe udostępniają organom ścigania szeroką wiedzę na temat osoby, która wykorzystała dane konto dla celów przestępczych, w tym jego pełne dane rejestracyjne w postaci danych osobowych i teleadresowych, adresu poczty elektronicznej podanego podczas rejestracji, analogicznie numeru telefonu a także adresu IP, wykorzystanego zarówno podczas rejestracji użytkownika jak również podczas zamieszczania ogłoszenia na platformie sprzedażowej. Analogiczne dane udostępniane są przez operatorów portali i komunikatorów społecznościowych, które nadto – na żądanie[315] – udostępniają historie rozmów prowadzonych za ich pośrednictwem wraz z plikami w postaci zdjęć czy nagrań wideo, co bywa kluczowe w przypadku przestępstw o charakterze seksualnym[316]. Powyżej wskazane okoliczności wyraźnie wskazują, że pozyskanie danych telekomunikacyjnych od operatorów sieci komórkowych jak również od administratorów poczty elektronicznej czy innych usługodawców bywa kluczowym zabiegiem z punktu widzenia wykrycia sprawcy cyberprzestępstwa. Wyraźnie jednak zaznaczyć należy, iż dotarcie do pełnych danych użytkownika końcowego bywa mozolnym, trudnym i długotrwałym procesem, niekiedy nazywanym również „łańcuchowym", albowiem w zdecydowanej większości przypadków po uzyskaniu danych dotyczących użytkownika końcowego niemalże natychmiast – w celu zabezpieczenia danych – konieczne jest sporządzenie kolejnego postanowienia o żądaniu wydania rzeczy w tym zakresie oraz uzyskanie kolejnych informacji o sprawcy. Tylko natychmiastowe, skrupulatne i rzetelne działanie organów ściągania pozwoli na uzyskanie pełnych danych dotyczących cyberprzestępcy, a w konsekwencji ustalenie jego tożsamości.

W zakresie omawianej materii warte uwagi jest również wskazanie na niejako szczególną formę postanowienia o żądaniu rzeczy, a raczej na specjalną formę jego ekspedycji w przypadkach, w których jest ono adresowane do większości usługodawców zajmujących się platformami sprzedażowymi, w tym Allegro.pl Sp. z o. o. oraz Grupa Olx.pl Sp. z o.o. jak również do operatorów portali społecznościowych takich jak Facebook, administrowanych przez podmioty zagraniczne. Co prawda, ustawodawca przewiduje, iż do wyłącznej dyspozycji prokuratora pozostaje sporządzenie postanowienia o żądaniu wydania rzeczy, wyłączając w ten sposób kwestię tą z zasięgu chociażby funkcjonariuszy Policji, którzy *de facto* prowadzą

[315] W drodze postanowienia o żądaniu wydania rzeczy

[316] Szerzej: M. Rogalski, *Udostępnianie danych telekomunikacyjnych sądom i prokuratorom*, Prokuratura i Prawo 2015, nr 12

zdecydowaną większość takich postępowań przygotowawczych, niemniej jednak w przypadku rzeczonych operatorów w praktyce przyjęło się, iż są one dostarczane adresatom w formie elektronicznej za pośrednictwem właściwej jednostki policji. Okoliczność ta bezpośrednio implikuje konieczność stwierdzenia, iż funkcjonariusze w związku z tym w pewien sposób uczestniczą w procedurze pozyskania danych telekomunikacyjnych, a co więcej – odpowiedź w tym zakresie przekazywana jest bezpośrednio policji, która wówczas niezwłocznie może podjąć się ich analizy. Analizując kwestię sposobu przekazywania postanowienia o żądaniu wydania rzeczy, nie sposób nie wspomnieć również o pewnej innowacyjności w tym zakresie podyktowanej rozwojem technologicznym oraz związaną z tym chęcią i możliwością usprawnienia i przyspieszenia, zwłaszcza procedur karnych. Dotychczas w sposób elektroniczny, za pomocą specjalnie opracowanego oprogramowania, wypełniając właściwie przygotowany formularz, możliwe było zwrócenie się do operatora sieci komórkowej P4 Sp. z o.o. (Play). Wówczas, za pośrednictwem tego samego programu, dane telekomunikacyjne również nadsyłane były w formie elektronicznej.

Na początku 2022 r. w związku z wprowadzeniem dla wszystkich jednostek prokuratury na terenie kraju nowego systemu baz danych ProkSys, udostępniono również innowacyjne metody przesyłania postanowień o żądaniu wydania rzeczy do wszystkich operatorów sieci komórkowych, które jednocześnie zastrzegły, iż wyłącznie na zapytania przesłane w tej formie będą udzielać skutecznych odpowiedzi, które z kolei również udostępniane będą na tej platformie. Za pomocą tego systemu teleinformatycznego, generowana jest niemal automatycznie treść decyzji. Program automatycznie pobiera dane z systemu ProkSys dotyczące danej sprawy, wymagane jest wyłącznie w zasadzie wpisanie sygnatury sprawy, zaś jej przedmiot oraz kwalifikacja prawna objęta zakresem tego postępowania, uzupełniana jest automatycznie. Następnie przy wykorzystaniu przygotowanego przez system dokumentu i formularza prokurator uzupełnia dane, w zakresie których zachodzi konieczność uzyskania informacji. Na tej podstawie generowany jest dokument, którego najistotniejszym elementem jest kod QR, na podstawie którego operatorzy udostępniają właściwe dane. Nie ma wątpliwości co do tego, iż rzeczone zabiegi w sposób bezpośredni wpływają zarówno na tempo prowadzonego postępowania przygotowawczego jak również na jego jakość. Rozwój technologiczny pozwala na udostępnienie organom ścigania takich instrumentów wykorzystujących nowe technologie, dzięki którym możliwe jest niemalże natychmiastowe uzyskanie danych retencyjnych, w przypadku których czas bywa niezwykle istotnym czynnikiem wpływającym bezpośrednio na możliwość wykrycia sprawcy cyberprzestępstwa.

Przed zmianami w tym zakresie, postanowienia jak i odpowiedzi na żądania przesyłane były pocztą tradycyjną, co ze względów oczywistych oznaczało, iż niejednokrotnie oczekiwanie na odpowiedź mogło trwać nawet kilka miesięcy. Nowoczesny system zabezpieczenia danych telekomunikacyjnych umożliwia natomiast ich uzyskanie nawet w ciągu kilku dni. Różnica, jak widać, jest znaczna i nie ma wątpliwości co do tego, że bezpośrednio wpływa zarówno na czas trwania postępowania i wykrycie sprawcy, jak również na ekonomikę procesową.

2.4. Reasumpcja materiału dowodowego

Po uzyskaniu od operatora telekomunikacyjnego i administratorów domen internetowych odpowiedzi na uprzednio skierowane postanowienie o żądaniu wydania rzeczy w postaci danych abonenta, wykazu połączeń, adresów IP, danych rejestracyjnych i ewentualnie innych danych telekomunikacyjnych, organy ścigania współpracując ze sobą mogą podjąć próbę identyfikacji użytkownika końcowego[317]. Jak wyżej wskazywano proces pozyskania i zabezpieczenia tych danych bywa niezwykle skomplikowany i długotrwały, niemniej jednak sposoby analizy uzyskanych danych retencyjnych przez organy ścigania jak również kwestia narzędzi udostępnionych dla skutecznej analizy z praktycznego punktu widzenia zostanie omówiona w kolejnym rozdziale, albowiem jest to na tyle złożona materia, że wymaga odrębnego omówienia. Wskazać jedynie należy, iż na podstawie uzyskanych danych telekomunikacyjnych można uzyskać informację na temat trzech zagadnień, tj. kim był użytkownik Internetu, gdzie wówczas się znajdował oraz z jakiego urządzenia w tym celu korzystał. Na podstawie poczynionych w ten sposób ustaleń zachodzi konieczność podjęcia decyzji co do dalszego toku postępowania, przy czym wskazać należy, iż kwestia ta może przedstawiać się następująco:

1. brak możliwości zidentyfikowania sprawcy za pomocą ustalonych danych telekomunikacyjnych, najczęściej z powodu wykorzystania przez sprawcę technik maskujących ruch w sieci lub ukrywających lokalizację BTS – wówczas wydawana jest decyzja o merytorycznym zakończeniu postępowania na zasadzie art. 322 § 1 k.p.k., tj. umorzenie postępowania przygotowawczego z uwagi na niewykrycie sprawcy czynu zabronionego;
2. w przypadku, w którym dotychczas zgromadzony materiał dowodowy oraz dane zebrane w toku postępowania uzasadniają dostatecznie podejrzenie, iż czyn objęty

[317] Szerzej: P. Opitek, *Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych,* Prokuratura i Prawo 2018/7-8/65-85; czynności te zazwyczaj wykonywane są przez analityków kryminalnych – szerzej w tym zakresie: S. Godlewska, *Analiza kryminalna w postępowaniu karnym,* Prokuratura i Prawo 2022/3/55-72

zakresem tego postępowania popełniła określona osoba – w myśl art. 313 § 1 k.p.k. sporządzane jest postanowienie o przedstawieniu zarzutów, które ogłaszane jest podejrzanemu i przesłuchuje się go, a następnie podejmuje czynności zmierzające do zakończenia postępowania poprzez skierowanie aktu oskarżenia do właściwego sądu;

3. jeśli zgromadzone informacje nie pozwalają jednak na bezsporne ustalenie, kto w rzeczywistości dopuścił się popełnienia cyberprzestępstwa, a wyczerpane zostały możliwości dowodowe w zakresie pozyskania danych telekomunikacyjnych, organy ścigania mają wówczas możliwość przeprowadzenia czynności procesowych z tzw. osobowych źródeł dowodowych, tj. przesłuchania świadków.

2.5.Osobowe źródła dowodowe

Jak wyżej wskazano decyzja o wyborze kolejnego etapu postępowania przygotowawczego bezapelacyjnie należy do organów ścigania i bezpośrednio podyktowana jest całokształtem dotychczas zgromadzonego materiału dowodowego w powiązaniu z ustalonym stanem faktycznym. Niekiedy poczynione w toku postępowania przygotowawczego ustalenia nie pozwalają na bezsporne ustalenie tożsamości sprawcy przestępstwa, natomiast możliwe jest wytypowanie tzw. osób podejrzewanych, co do których zachodzi podejrzenie, iż mogłyby być sprawcami cyberprzestępstwa, niemniej jednak nie przybiera ono stadium dostatecznie uzasadnionego. Wówczas, zanim prowadzący postępowanie w formie dochodzenia lub śledztwa, może podjąć decyzję o przeprowadzeniu przesłuchania osób, o których wspomniano powyżej. Zasygnalizować jedynie należy, iż odmiennie do czynności sporządzenia postanowienia o żądaniu wydania rzeczy, przesłuchania mogą zostać przeprowadzone przez funkcjonariuszy Policji lub inne organy postępowania przygotowawczego, albowiem czynność ta zarówno w dochodzeniu jak i śledztwie co do zasady nie jest zastrzeżona do wyłącznej kompetencji prokuratora.

W zdecydowanej większości przypadków organy ścigania podejmują decyzję o wykonaniu czynności procesowych z wyżej wskazanymi osobami w sytuacjach, w których ustalono ich jako użytkowników końcowych, tj. zarejestrowano na ich dane numer telefonu lub adres poczty elektronicznej, ewentualnie skorzystano z należącej do nich sieci internetowej bądź dla celów przestępczych wykorzystano rachunek bankowy, którego dysponentem jest konkretna osoba. W kwestiach formalnych wskazać należy, iż osoby takie przesłuchiwane są w charakterze świadków, z tym zastrzeżeniem, iż przed przystąpieniem do przesłuchania poucza się ich o treści art. 183 k.p.k., umożliwiającego uchylenie się od odpowiedzi na pytania

bądź odmowy składania zeznań w sytuacji, gdyby odpowiedź mogłaby narazić świadka na odpowiedzialność karną jego lub osobę dla niego najbliższą. Jest to o tyle istotne zastrzeżenie, iż pouczenie to adresowane jest co do zasady wyłącznie do tzw. osób podejrzewanych, co do których chociażby w niewielkim stopniu zachodzi prawdopodobieństwo przestępczego działania. Nadto, niezależnie od powyższego, świadków poucza się o treści art. 233 § 1 k.k. to jest o odpowiedzialności karnej za składanie fałszywych zeznań, czego nie czyni się w przypadku przesłuchiwania podejrzanego, czyli osoby będącej formalnie po ogłoszeniu postanowienia o przedstawieniu zarzutów.

W toku postępowania przygotowawczego wykonanie czynności procesowych z udziałem świadków zawęża krąg osób podejrzewanych lub też treść zeznań konkretnego świadka bezpośrednio wskazuje na jego sprawstwo. Niemniej jednak zdarzają się również sytuacje, w których okazuje się, iż dane konkretnej osoby wyłącznie wykorzystano dla celów przestępczych poprzez tzw. kradzież tożsamości[318]. Bywa również tak, iż sprawca skorzystał z niezabezpieczonej odpowiednio sieci internetowej świadka, który w rzeczywistości w żaden sposób nie brał udziału w przestępczym procederze. Bardzo popularnym zjawiskiem jest również metoda działania na tzw. „słupa", gdzie karty SIM rejestrowane są na przypadkowe osoby, podobnie jak umowy o rachunki bankowe zawierane w ten sam sposób. Okoliczności te uwidaczniane są właśnie na etapie przesłuchiwania świadków po uprzednio ustalonych danych retencyjnych. Reasumując kwestię algorytmu skrupulatnie przygotowywanego przez organy ścigania, ponownie wskazać należy, iż powinien być on doprecyzowywany w odniesieniu do konkretnego stanu faktycznego, albowiem słusznie w praktyce się wskazuje, iż nie ma dwóch identycznych przestępstw, a wyłącznie kompletny materiał dowodowy w powiązaniu z rzetelnie ustalonymi okolicznościami faktycznymi pozwoli na osiągnięcie celów postępowania i wykrycie oraz pociągnięcie do odpowiedzialności karnej sprawcy przestępstwa.

[318] Szerzej: P. Litwiński, *Naruszenia bezpieczeństwa danych osobowych obejmujących numer PESEL – analiza ryzyka,* [w:] A. Matan (red.) *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza,* Wolters Kluwer, 2022 oraz K. Kamińska, *Zjawisko kradzieży tożsamości – aspekty prawne i kryminologiczne* [w:] D. Dajnowicz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E.W. Pływaczewski (red.), *Przestępczość XXI wieku. Szanse i wyzwania dla kryminologii*, 2020

Rozdział V

Sztuczna inteligencja a przyszłość zawodów prawniczych

Współcześnie obraz nowych technologii i konsekwencje z tego wynikające bywają nieprawdopodobnie zaskakujące, albowiem okazuje się, iż wszystkie sektory gospodarki wspierane są przez komunikację elektroniczną, a nowe technologie same w sobie stały się najbardziej pożądaną z dostępnych usług. Nie pozostawia wątpliwości fakt, iż nierozerwalnym aspektem postępu technologicznego jest sztuczna inteligencja, która na przestrzeni lat zyskuje coraz to większą popularność, docierając do wszystkich dziedzin życia, w tym publicznego[319], społecznego a zwłaszcza ekonomicznego. Możliwość wykorzystania sztucznej inteligencji przy jednoczesnym zminimalizowaniu czynnika czasu oraz zwiększeniu efektywności, a w konsekwencji również zysku ekonomicznego rozpatrywanego przez pryzmat wielu korzyści sprawia, iż możliwości sztucznej inteligencji zdają się być bardzo obiecujące zwłaszcza dla dużych przedsiębiorców.

O ile fakt dotarcia tej formy nowych technologii do wielu sektorów gospodarki w zasadzie nie budzi wątpliwości, o tyle kwestia ich przyjęcia wśród działalności prawniczych wzbudza kontrowersje i wątpliwości co do przyszłości tej grupy zawodowej. W związku z tym pojawiają się liczne pytania, w tym między innymi: która grupa prawników jest najbardziej zagrożona, w której z grup narzędzia wykorzystujące sztuczną inteligencję mógłby faktyczne stać się użyteczne, w jaki sposób prawnicy mogliby wykorzystać takie narzędzia i najważniejsze – czy uczenie maszynowe jest w stanie zastąpić prawnika uwzględniając zwłaszcza charakter tej dziedziny naukowej, tj. nauk prawnych sklasyfikowanych jako nauki społeczne. Wiele wątpliwości wzbudza również kwestia odpowiedzialności za działania podejmowane w ramach sztucznej inteligencji. Niezależnie od powyższego, nie ma wątpliwości co do tego, iż fenomen sztucznej inteligencji jest dynamiczny, szybko rozwijający się, ulegający nieustannym udoskonaleniom[320]. Dla potwierdzenia tej tezy wskazać jedynie należy, iż szacuje się, iż rynek sztucznej inteligencji w 2019 r. był wart 27,3 mld dolarów, podczas gdy do 2026 r. będzie już wart blisko 267 mld dolarów[321].

[319] Szerzej na temat zautomatyzowanego podejmowania decyzji w administracji publicznej: A. Monarcha-Matlak, *Automated decision-making in public administration,* Procedia Computer Science 192 (2021): 2077-2084

[320] Szerzej: I. Jankowska-Proch, *Odpowiedzialność karna a działalność autonomicznych robotów. Wyzwania prawne i etyczne w polskim i światowym dyskursie naukowym* [w:] P. Chmielnicki (red.), D. Minich (red.), *Prawo jako projekt przyszłości*, 2022

[321] R.E. Long, *Artificial intelligence liability: the rules are changing*, https://blogs.lse.ac.uk/businessreview/2021/08/16/artificial-intelligence-liability-the-rules-are-changing/

1. Definicja sztucznej inteligencji oraz jej rodzaje

Na tle pierwszego rozdziału rozprawy wyczerpująco przeanalizowano i omówiono szeroką siatkę pojęciową dotyczącą definicji związanych zarówno bezpośrednio jak i pośrednio ze sferą nowych technologii oraz komunikacji elektronicznej. Nie bez powodu pominięto wówczas dogłębne rozważania na temat pojęcia sztucznej inteligencji, decydując, iż kwestia ta wymaga odrębnej uwagi.

W celu możliwie największego ujednolicenia omawianych kwestii oraz w celu zapewnienia precyzji omawianych zagadnień, poniżej przedstawione zostaną jedynie najważniejsze elementy z zakresu materii teoretycznej, zwłaszcza kluczowe i najbardziej trafne definicje pojęcia sztucznej inteligencji, w tym aspekty poruszane na gruncie prawa międzynarodowego (także przez organy Unii Europejskiej), a nadto rodzaje sztucznej inteligencji. Analiza kwestii teoretycznych zdaje się być ważnym przedmiotem rozważań, niemniej jednak nie na tyle doniosłym, aby skupiać na nim główny ciężar badań, zwłaszcza mając na względzie interesującą, a przede wszystkim wątpliwą i problematyczną sferę dotyczącą szeroko rozumianej sztucznej inteligencji w praktyce, odpowiedzialności wyrządzonej przy jej wykorzystaniu jak również możliwości jej zastosowania na rynku zawodów prawniczych oraz organów ścigania i wymiaru sprawiedliwości. Pojęcie sztucznej inteligencji w XXI wieku jest bardzo szeroko wykorzystywane, nie tylko w sferze naukowej, ale również publicystycznej i politycznej. Poszukując genezy pojęcia sztucznej inteligencji, powołać się bez wątpienia należy na definicję, którą posłużył się w 1955 r. John McCarthy. Według niego pierwotnie pojęcie to miało oznaczać proces, który sprawia, że maszyna zachowuje się w sposób, który nazwalibyśmy inteligentnym, gdyby w ten sposób zachowywał się człowiek. Niemniej jednak nieustannie dostrzegalny rozwój technologiczny podyktował bezpośrednio konieczność zmodyfikowania tej definicji i dostosowania jej do aktualnej rzeczywistości oraz możliwości jakie dostarczają nowe technologie.

Nie sposób uznać, iż aktualnie dostępna jest idealnie opracowana definicja sztucznej inteligencji, zwłaszcza taka, przy wykorzystaniu której możliwe byłoby wprowadzenie regulacji prawnych w tej materii. W pierwszej kolejności wyraźnie zaznaczyć należy, iż dotychczas w ustawodawstwie krajowym nie wypracowano definicji legalnej tego pojęcia. W piśmiennictwie podnosi się, iż Sztuczna Inteligencja (Artificial Intelligence, AI) to dziedzina nauki zajmująca się rozwiązywaniem zagadnień efektywnie niealgorytmizowalnych w oparciu

(dostęp: 07.02.2023 r.)

o modelowanie wiedzy. Pomimo funkcjonowania w obrocie prawnym na szczeblu międzynarodowym wielu definicji rzeczonego pojęcia, w pełni celowe i uzasadnione zdaje się być w pierwszej kolejności przytoczenie znaczenia opracowanego przez z Grupę Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (powołaną przez Komisję Europejską w 2018 r.). Uzasadnia to przede wszystkim fakt, iż Unia Europejska jest podmiotem, który obecnie wyznacza standardy regionalne w dziedzinie sztucznej inteligencji (zwanej dalej SI)[322]. W myśl tej definicji systemy SI to: oprogramowania komputerowe (i ewentualnie również sprzęt komputerowy) stworzone przez człowieka, które, biorąc pod uwagę założony cel, działają w wymiarze fizycznym lub cyfrowym poprzez postrzeganie ich otoczenia dzięki gromadzeniu danych, interpretacji zebranych ustrukturyzowanych lub nieustrukturyzowanych danych, rozumowaniu na podstawie wiedzy lub przetwarzaniu informacji pochodzących z tych danych oraz podejmowaniu decyzji w sprawie najlepszych działań, które należy podjąć w celu osiągnięcia określonego celu[323]. Systemy SI mogą wykorzystywać symboliczne reguły albo uczyć się modelu numerycznego, a także dostosowywać swoje zachowanie, analizując wpływ ich poprzednich działań na otoczenie. W przygotowanym przez specjalną komisję przy organach UE dokumencie „Sztuczna inteligencja dla Europy"[324] zawarta jest definicja sztucznej inteligencji. Według niej „sztuczna inteligencja odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów". W dniu 9 lutego 2020 roku Komisja Europejska wydała „Białą Księgę w sprawie sztucznej inteligencji"[325], w której zostały określone mechanizmy, przy zastosowaniu których minimalizowane będą różnego rodzaju ryzyka, które wiążą się z dynamicznym rozwojem sztucznej inteligencji na świecie. W Księdze wskazana została niezwykła przydatność zastosowania sztucznej inteligencji w sektorach publicznych.

Upraszczając, przyjąć zatem należy, iż sztuczna inteligencja to techniczne rozwiązanie (co do zasady program komputerowy) wykonujące czynności będące zazwyczaj domeną ludzi, szczególnie wymagających użycia ludzkiego intelektu[326]. Z jednej strony wykorzystywanie

[322] R. Rejmaniak, Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego, Roczniki Nauk Prawnych Tom XXXI, numer 3-2021, s. 97

[323] Szerzej zob. np. C. Amato, *Traditional Liability Requirements and New Sources of Damages* [w:] *Liability for Artificial Intelligence and the Internet of Things*, red. S. Lohsse, R. Schulze, D. Staudenmayer, Baden-Baden 2019, s. 77 i n.

[324] Komunikat Komisji Europejskiej z dnia 25 kwietnia 2018 roku , Sztuczna Inteligencja dla Europy, COM (2018) 237 final

[325] Biała Księga w sprawie sztucznej inteligencji. Europejskie Podejście do doskonałości i zaufania. Komisja Europejska, 19 lutego 2020 r. COM (2020) 65 final

[326] T. Zalewski, *Prawo Sztucznej Inteligencji*, C.H. Beck, Warszawa 2020, s. 5

systemów SI w wielu sferach rzeczywistości społecznej, np. w służbie zdrowia, w przemyśle, w usługach, w sektorze publicznym czy w energetyce, usprawnia pracę i przynosi wielkie korzyści. Z drugiej jednak, dostrzegalne są też zagrożenia niesione przez upowszechnianie się sztucznej inteligencji[327]. Przyjąć należy, iż elementem konstytutywnym każdego rodzaju inteligencji jest zdolność do uczenia się i zdolność do samodzielnego rozwiązywania problemów. Jedynym z wyznaczników „inteligencji" sztucznej inteligencji powinna być zatem jej zdolność do uczenia się[328]. Zdolność uczenia się jest realizowana w ramach sztucznej inteligencji poprzez wykorzystanie technik programowania polegających na przetwarzaniu danych.

Reasumując wyżej poczynione ustalenia przyjąć należy, iż sztuczna inteligencja to system, który pozwala na wykonywanie zadań wymagających procesu uczenia się i uwzględniania nowych okoliczności w toku rozwiązywania danego problemu i który może w różnym stopniu – w zależności od konfiguracji – działać autonomicznie oraz wchodzić w interakcję z otoczeniem[329]. Ważną cechą sztucznej inteligencji, odróżniającą ją od innych systemów jest jej autonomiczność rozumiana jako umiejętność samodzielnego działania bez ingerencji człowieka. Jest to cecha stopniowalna, począwszy od całkowitej niezależności kończąc na tylko częściowej możliwości działania bez pomocy człowieka. Odnosząc się do cechy konstytutywnej sztucznej inteligencji, tj. zdolności do uczenia się zaznaczyć wyraźnie należy, iż wykorzystywanie zewnętrznych danych empirycznych w celu tworzenia i aktualizacji podstaw dla udoskonalonego działania na podobnych danych w przyszłości oraz wyrażania tych podstaw w zrozumiałej i symbolicznej postaci – tzw. uczenie się maszynowe[330]. Jedną ze współcześnie najbardziej popularnych technik jest uczenie głębokie oparte o wiele warstw sztucznych sieci neuronowych. W przypadku podjęcia próby regulacji prawnych dotyczących sztucznej inteligencji, celowe było opisowe opracowanie definicji, przy odpowiednim uzupełnieniu jej o pojęcia informatyczne, zaś same regulacje powinny odnosić się bezpośrednio do szeroko rozumianego ryzyka prawnego oraz ewentualnych kwestii odpowiedzialności wyrządzonej w związku z wykorzystaniem narzędzi opartych o działanie

[327] W. Filipkowski, *Prawo karne wobec sztucznej inteligencji, [w:] Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa: Wydawnictwo C.H. Beck 2020, s. 124-125
[328] T. Zalewski, *Prawo Sztucznej Inteligencji*, C.H. Beck, Warszawa 2020, s. 4
[329] Ibidem,. s. 14
[330]R. Rejmaniak, *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, Roczniki Nauk Prawnych Tom XXXI, numer 3-2021, s. 100

sztucznej inteligencji[331]. Nadmienić jedynie należy, iż w literaturze przedmiotu niejednokrotnie wskazuje się na funkcjonalny aspekt sztucznej inteligencji, zgodnie z którym, jej celem jest automatyzowanie intelektualnych działań człowieka w zakresie wnioskowania, kojarzenia i doboru informacji[332].

1.1. Rodzaje sztucznej inteligencji

Zarówno na gruncie rozważań podejmowanych w obszarze prawa międzynarodowego, w tym przede wszystkim przez organy Unii Europejskiej, jak również w piśmiennictwie wskazuje się na dwa podejścia do zagadnień bezpośrednio dotyczących sztucznej inteligencji. Wyróżnia się tzw. słabą sztuczną inteligencję (tzw. *weak AI*) oraz silną sztuczną inteligencję (tzw. *strong AI*). Przyjmuje się, iż pojęcia słabej sztucznej inteligencji używa się do opisu systemów komputerowych analizujących dane, które są następnie używane do podejmowania pewnych decyzji, co stanowi odtworzenie funkcjonowania inteligencji człowieka. Można zatem wskazać, że słaba sztuczna inteligencja to taka, która w relacjach w obrocie gospodarczym i prawnym działa samodzielnie. Samodzielność oznacza natomiast posiadanie wbudowanych algorytmów wyposażonych w zdolność samouczenia się, co z kolei implikuje fakt autonomiczności jej działań i faktycznej pozycji, podlegając jedynie maksymalnie ograniczonej, następczej kontroli człowieka lub też nie podlegając wcale takiej kontroli[333].

Silna inteligencja dotyczy natomiast sytuacji, w której odpowiednio zaprogramowany komputer byłby w istotny sposób równoważny mózgowi, a więc posiadałby elementy ludzkiej inteligencji. Możliwe byłoby wobec tego konstruowanie programów „samouczących się", takich jak modele sieci neuronowych oraz opracowywanie procedur rozwiązywania problemów poprzez „uczenie" takich programów, a następnie uzyskiwanie od nich odpowiedzi na „pytania"[334]. Zasygnalizować nadto należy, że silna sztuczna inteligencja obejmuje dwa typy sztucznej inteligencji: ogólną sztuczną inteligencję (*Artificial General Intelligence – AGI*) i sztuczną superinteligencję (*Artificial Super Intelligence – ASI*). AGI to system posiadający samoświadomość. Potrafi rozwiązywać problemy, a nawet planować przyszłość. ASI to system przewyższający ludzkie zdolności. Do tej pory nie zostały stworzone systemy „silnej sztucznej inteligencji" rozumianej jako system zdolny do całkowicie samodzielnego myślenia. Sztucznej

[331] HLEG AI Definition 2018: The European Commission's High-Level Expert Group on Artificial Intelligence, *A definition of* AI*: Main capabilities and scientific disciplines*. *Definition developed for the purpose of the deliverables of the High-Level Expert Group on* AI, Brussels 2018, tłum. za T. Zalewski, *Definicja...*, s. 8.
[332] J. Janowski, *Trendy cywilizacji informacyjnej. Nowy technototalitarny porządek świata*, Warszawa 2019, s. 43.
[333] B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), *Prawo* sztucznej inteligencji *i nowych technologii,* Wolters Kluwer, Warszawa 2021, s. 119
[334]K. Różanowski, *Sztuczna inteligencja: Rozwój, szanse, zagrożenia,* s. 111-112

inteligencji nie można utożsamiać z prostymi algorytmami, albowiem oprócz wykonywania przypisanych jej zadań ma ona w swoim genie także dążność do ciągłego udoskonalania się i wyboru najefektywniejszych rezultatów na przyszłość[335].

Reasumując omawianie aspektów teoretycznych, zasygnalizować należy, iż nazewnictwo w przypadku wyróżnionych rodzajów sztucznej inteligencji uznać należy za nietrafne. Niezrozumiałe jest bowiem przypisanie przymiotnika słabej sztucznej inteligencji, która zdaje się być nieprawdopodobną szansą dla wielu sektorów gospodarki i która aktualnie jest szeroko wykorzystywana w wielu sektorach, również publicznych. Zdaje się, że zdecydowanie bardziej trafnym określeniem byłoby uznanie tego rodzaju sztucznej inteligencji jako „wąskiej" lub też pozostawienie tego rodzaju bez opisu za pomocą określenia, pozostawiając jednakże w obrocie sformułowanie silnej sztucznej inteligencji, co pozwoliłoby w wystarczający sposób odróżnić te kwestie.

2. Odpowiedzialność za szkody wyrządzone sztuczną inteligencją

Dokonując analizy aspektów teoretyczno-prawnych dotyczących sztucznej inteligencji należy zwrócić szczególną uwagę na jeszcze jeden element. Z uwagi na coraz szersze wykorzystywanie narzędzi opartych na działaniu sztucznej inteligencji w wielu sektorach gospodarki oraz wielu sferach życia społecznego, nieunikniona była konieczność uregulowania prawnego tejże kwestii, zwłaszcza z punktu widzenia odpowiedzialności za szkody wyrządzone w związku z funkcjonowaniem sztucznej inteligencji. Nie sposób nie zgodzić się, iż kwestia ta budzi w zasadzie od początku bytu sztucznej inteligencji najwięcej wątpliwości, problemów zarówno w wymiarze teoretycznym, ale również praktycznym. Okoliczność ta bezpośrednio implikowała konieczność wprowadzenia rozwiązań prawnych zarówno w porządku krajowym, jak również, a w zasadzie przede wszystkim – na szczeblu europejskim.

W polskim ustawodawstwie w tym zakresie podjęto uchwałę nr 196 Rady Ministrów z dnia 28 grudnia 2020 roku w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od 2020 r."[336]. Akt ten wskazuje wprost na działania, które Polska powinna wdrożyć i cele, które powinna osiągnąć w perspektywie podzielonej na trzy okresy, to jest do 2024 roku, do 2027 roku oraz po 2027 r. Kwestie te omówiono w odniesieniu do

[335] P. Staszczyk, *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna*, EPS 2022/6/24-30

[336] Uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 roku w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020", Monitor Polski 2021 poz. 23

kluczowych sektorów, to jest społeczeństwa, nauki, edukacji, współpracy międzynarodowej, innowacyjnych firm oraz sektora publicznego. W tym dokumencie tym wskazano, iż za sprawą sztucznej inteligencji za około 100 dotychczasowych miejsc pracy pojawi się 130 nowych, a do 2030 roku aż 49% czasu w Polsce może zostać zautomatyzowane przy wykorzystaniu już istniejących technologii. Choć postulaty te zdają się być bardzo daleko idące i możliwe do osiągnięcia w długoterminowej perspektywie, to z nadzieją należy ocenić je pozytywnie, uwzględniając przede wszystkim znamienny wpływ nowych technologii, a w konsekwencji również sztucznej inteligencji. Jest to zdecydowanie możliwe do osiągnięcia, biorąc pod uwagę zwłaszcza fakt, iż dla priorytetowych sektorów gospodarki i wskazanych dla zastosowań AI korzyści z wdrażania AI to około 2,65% PKB.

Z ostrożnością spojrzeć natomiast należy na cel długoterminowy, zgodnie z którym Polska znajduje się w pierwszej dziesiątce krajów najbardziej gotowych do wdrożenia AI (AI Readiness Index)[337]. Według danych ogłoszonych na zakończenie 2021 roku według ww. rankingu, który obejmuje 160 krajów według stopnia przygotowania rządów do wykorzystania sztucznej inteligencji w usługach publicznych, wynik indeksu dla Polski określony został na poziomie 62,50/100 zaś w ogólnym rankingu Polska zajmowała wówczas 35 miejsce. Państwa sąsiedzkie takie jak Czechy – 29 miejsce, Niemcy – 7 miejsce, Białoruś – 73 miejsce. Dla zobrazowania postępu w zakresie wykorzystania sztucznej inteligencji w możliwie najszerszym ujęciu celowe zdaje się być również wskazanie na wyniki rzeczonego rankingu w 2022 r.[338]. Wówczas Polska została ulokowana na 36 miejscu ogólnego rankingu, uzyskując wynik na poziomie 62,65, uzyskując największą punktację w zakresie filaru danych i infrastruktury.

Na czele rankingu zarówno w 2021 r., jak i 2022 r. znalazły się Stany Zjednoczone, tuż za nimi Singapur, a trzecie miejsce uzyskała Wielka Brytania. W 2021 roku prawie 40% krajów biorących udział w rankingu opublikowało lub opracowuje krajowe strategie dotyczące sztucznej inteligencji. Co ciekawe, kraje Azji Wschodniej stanowiły wówczas niemalże jedną czwartą z 20 najwyżej sklasyfikowanych krajów. Globalne zainteresowanie sztuczną inteligencją pojawia się w trakcie szerszego zwrotu w kierunku cyfrowego rządu, w dużej mierze pobudzonego środkami dystansowania społecznego wdrożonymi w odpowiedzi na pandemię koronawirusa. Krajowe strategie sztucznej inteligencji pozostają jednak skoncentrowane w krajach globalnej północy, co świadczy o pogłębiającym się podziale w globalnej gotowości sztucznej inteligencji. W 2022 roku dostrzeżono zmiany regionalne: po raz

[338] https://www.oxfordinsights.com/government-ai-readiness-index-2022 (dostęp: 06.02.2022 r.)

pierwszy kraje Europy Zachodniej stanowią mniej niż połowę pierwszej dziesiątki, podczas gdy trzy kraje Azji Wschodniej zajmują czołowe pozycje.

Nie pozostawia wątpliwości fakt, iż rozwiązania prawne dotyczące sztucznej inteligencji, a zwłaszcza jej odpowiedzialności za wyrządzone szkody, powinny zostać uwzględnione w prawodawstwie unijnym[339]. Początki prawodawstwa europejskiego w zakresie uregulowań dotyczących *stricte* sztucznej inteligencji rozpoczęły się wraz z przyjęciem Rezolucji Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierającej zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki. Ten stanowiący źródło prawa miękkiego (*soft law*) akt był pierwszą regulacją, który ukierunkował dyskusję nad odpowiedzialnością w obszarze sztucznej inteligencji w Unii Europejskiej[340]. Znamienny w tym zakresie okazać się może również projekt rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii Europejskiej z dnia 21 kwietnia 2021 r.[341] a także projekt Komisji Europejskiej dyrektywy w sprawie dostosowania przepisów dotyczących odpowiedzialności cywilnej pozaumownej do sztucznej inteligencji mający na celu harmonizację przepisów krajowych odnoszących się do odpowiedzialności za sztuczną inteligencje[342]. Kwestia odpowiedzialności za sztuczną inteligencję, zwłaszcza w odniesieniu do szkód spowodowanych przez systemy sztucznej inteligencji jest bardzo złożonym i obszernym tematem, zdecydowanie wymagającym szczegółowej analizy, w związku z czym nie głównym punktem zainteresowania na kanwie przedmiotowych rozważań. Wskazać jedynie należy, iż Komisja Europejska zaproponowała harmonizację krajowych przepisów odnoszących się bezpośrednio do omawianej kwestii, a celem tych regulacji jest ułatwienie ofiarom potencjalnych szkód spowodowanych przez sztuczną inteligencję dochodzenia odszkodowanie. Celem dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję jest ustanowienie jednolitych przepisów dotyczących dostępu do informacji i zmniejszenia ciężaru dowodu w odniesieniu do szkód spowodowanych przez systemy sztucznej inteligencji, ustanowienie szerszej ochrony ofiar (zarówno osób fizycznych, jak i przedsiębiorstw) oraz wspieranie sektora sztucznej

[339] Szerzej: M. Jagielska, *Odpowiedzialność za* sztuczną inteligencję [w:] *Prawo* sztucznej inteligencji, red. L. Lai, M. Świerczyński, Warszawa 2020, s. 75.

[340] B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), *Prawo* sztucznej inteligencji *i nowych technologii,* Wolters Kluwer, Warszawa 2021, s. 119

[341] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206&from=PL(dostęp 07.02.2022 r.)

[342] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0496&qid=1665410785599 (dostęp: 07.02.2022 r.)

inteligencji poprzez zwiększenie gwarancji[343]. Niezależnie od powyższego, zgodzić się należy ze stanowiskiem coraz częściej podnoszonym w doktrynie, iż konieczność wprowadzenia specjalnych regulacji prawnych odnoszących się do odpowiedzialności za szkody wyrządzone przez sztuczną inteligencję, nie ma charakteru absolutnego, albowiem już teraz kwestię tejże odpowiedzialności można ustalić na podstawie przepisów ogólnych odnoszących się bezpośrednio do zasady winy i ryzyka, przy czym Istotne znaczenie dla przypisania odpowiedzialności może mieć także działanie lub zaniechanie samego użytkownika. Odpowiedzialność może zostać ograniczona w przypadku, gdy poszkodowany na przykład nie dokona aktualizacji istotnych z punktu widzenia bezpieczeństwa[344].

Podsumowując, nie ma wątpliwości, iż coraz szersze wykorzystanie sztucznej inteligencji determinuje konieczność wprowadzenia właściwych rozwiązań prawnych zarówno w porządku krajowym, jak również na szczeblu porządku europejskiego. Przeciwnicy takiego stanowiska wskazują, iż na tym etapie zastosowania sztucznej inteligencji kwestia ta jest pozbawiona sensu, co wynikać ma między innymi z faktu, iż rozwiązania wykorzystujące sztuczną inteligencję są dopiero wprowadzane na wiele płaszczyzn, co z kolei sprawia, że są to rozwiązania zmienne, dynamicznie i szybko rozwijające się[345], a powszechnie obowiązujące regulacje prawne można z powodzeniem dostosować do zaistniałych sytuacji. Nie sposób się zgodzić z takim stanowiskiem, albowiem niewątpliwie konieczne jest przyjęcie jednolitych regulacji prawnych pozwalających zarówno na tworzenie jak i wykorzystanie systemów sztucznej inteligencji w celu zapewnienia przede wszystkim rozwoju sztucznej inteligencji jak również ochrony praw podstawowych człowieka.

3. Przykłady wykorzystania sztucznej inteligencji w sektorze prywatnym

W związku z tym, iż sztuczna inteligencja staje się coraz bardziej popularnym i przede wszystkim dostępnym narzędziem, jej potencjał wykorzystywany jest w wielu dziedzinach życia społecznego. Z uwagi na obawę przed bezpieczeństwem wykorzystywanych technologii a także z uwagi na brak precyzyjnych regulacji dotyczących odpowiedzialności za szkody wyrządzone w związku z działaniem sztucznej inteligencji, omawiana technologia jest znacznie częściej wykorzystywana w sektorze prywatnym aniżeli w usługach publicznych, co przede

[343] R. Bujalski, *Odpowiedzialność za sztuczną inteligencję [Projekt UE] Komentarz praktyczny*, LEX, 2022
[344] K. Gorzkowska, *Odpowiedzialność za działania sztucznej inteligencji [w:]* A. Kidyba (red.), A. Olejniczak (red.)*, Nowoczesne technologie. Szansa czy zagrożenie dla funkcjonowania przedsiębiorców w obrocie prawnym i postępowaniach sądowych*, 2022
[345] P. Staszczyk, *Czy unijna regulacja odpowiedzialności za sztuczną inteligencję jest potrzebna*?, Europejski Przegląd Sądowy, 2022, s. 25 i nast.

wszystkim wynika z mniejszego ryzyka w przypadku ewentualnego wyrządzenia szkód w związku z wykorzystaniem urządzeń technologicznych opartych o działanie sztucznej inteligencji. Na potrzeby niniejszej rozprawy przywołać jedynie należy przykłady zastosowania narzędzi opartych o działanie sztucznej inteligencji w sektorze prywatnym w celu zobrazowania nieustannie rosnącego znaczenia tej technologii, niemniej jednak rozważania te mają wyłącznie charakter sygnalizacyjny, nie zaś kluczowy z punktu widzenia przedmiotu niniejszej rozprawy. Centrum uwagi skupione zostanie w obrębie zakresu wykorzystania sztucznej inteligencji wśród profesji prawniczych, a także postulatów w zakresie zwiększenia możliwości wykorzystania potencjału tej technologii wśród organów ścigania.

W pierwszej kolejności wskazać należy, iż niejednokrotnie w życiu codziennym operujemy z urządzeniami wykorzystującymi sztuczną inteligencję w szerokim ujęciu tego pojęcia, nie mając świadomości, iż z tego zakresu urządzeń korzystamy. Część społeczeństwa z uwagi na innowacyjny charakter tych narzędzi, obawia się ich używania, odczuwa obawę i ryzyko związane głównie z bezpieczeństwem takich transakcji. Jako pierwszy przykład wskazać można automatyczne rozpoznawanie mowy, czyli narzędzie, w które wyposażone jest większość urządzeń przenośnych, które *de facto* wykorzystywane są do komunikacji na odległość. Jest to funkcja wykorzystująca przetwarzanie języka naturalnego (NLP) do przetwarzania ludzkiej mowy na format pisemny. Funkcja ta głównie jest wykorzystywana na potrzeby przeprowadzenia wyszukiwania głosowego, np. Siri, lub zapewnienia większej dostępności usług wiadomości tekstowych. Nadto, coraz bardziej popularne, zwłaszcza w zakresie usług a precyzyjnie ujmując do kontaktów z klientami w wielu sferach działalności za pośrednictwem sieci teleinformatycznej, są internetowe chatboty jako forma obsługi klienta. Sztuczna inteligencja rozpoznaje temat rozmowy za pomocą uprzednio wprowadzonego uczenia maszynowego, a następnie odpowiada na często zadawane pytania. Przykłady obejmują boty do obsługi przesyłania wiadomości w serwisach handlu elektronicznego z wirtualnymi agentami, aplikacje do obsługi wiadomości, takie jak Facebook Messenger, oraz zadania zwykle wykonywane przez asystentów wirtualnych i głosowych. W aspekcie sprzedaży, istotną rolę odgrywa również tzw. sugerowanie sprzedaży, co ma wzmocnić efektywność oferowanych w tym zakresie usług. W tym przypadku algorytmy sztucznej inteligencji sugerują klientom inne produkty podczas dokonywania zakupów za pomocą różnych platform sprzedażowych. Kolejnym przykładem wykorzystania sztucznej inteligencji w życiu codziennym, nieustannie zyskującym na popularności z uwagi na sukcesywnie rosnący wzrost zainteresowania *social mediami*, jest

widzenie komputerowe. Jest to technologia wykorzystująca działanie sztucznej inteligencji, która dostarcza możliwości odczytania pewnych informacji z cyfrowych obrazów, najczęściej w postaci zdjęć, ale również nagrań wideo. Dzięki zastosowaniu sieci neuronowych widzenie komputerowe znajduje zastosowanie w znakowaniu zdjęć w mediach społecznościowych, obrazowaniu radiologicznym w służbie zdrowia i pojazdach autonomicznych w przemyśle motoryzacyjnym.

3.1. Automatyczne rozpoznawanie twarzy jako przykład zastosowania sztucznej inteligencji

Pomimo, iż narzędzie automatycznego rozpoznawania twarzy, które opartego jest bez wątpienia na działaniu algorytmów sztucznej inteligencji, *stricte* dotyczy sektora prywatnego, to jednak z uwagi na skalę jego wykorzystania zwłaszcza w sektorze usług bankowych, a także daleko idące konsekwencje z prawnokarnego punktu widzenia, celowe jest poddanie tej kwestii szczegółowej analizie, omawiając sposób faktycznego działania sztucznej inteligencji w tym zakresie. Automatyczne rozpoznawanie twarzy obecnie jest jednym z najpopularniejszych narzędzi, które bez wątpienia wykorzystuje potencjał nowych technologii. Technologia ta wiedzie zdecydowany prym w sektorze prywatnym, w zakresie urządzeń ogólnodostępnych, funkcjonując w obszarze codzienności społeczeństwa. Analiza zakresu pojęciowego rzeczonej technologii pozwala na sformułowanie praktycznej definicji automatycznego rozpoznawania twarzy. Przyjąć należy, iż jest to metoda wykorzystująca działanie nowych technologii, oparta na zautomatyzowanym mechanizmie weryfikacji osób w oparciu o analizę wizerunku twarzy. Algorytmy funkcjonujące w ramach sztucznej inteligencji na płaszczyźnie konkretnego obrazu wykrywają wizerunek twarzy, w odniesieniu do której ustalane są następnie charakterystyczne cechy, którymi najczęściej są konkretne odległości między odpowiednio wytypowanymi punktami. Kolejnym ustalane są cechy twarzy (charakterystyczne punkty, odległości między punktami), a kolejnym etapem jest rozpoznanie osoby (bądź brak jej rozpoznania) w wyniku porównania ustalonych cech z bazą wzorcową[346]. Identyfikacja osób w oparciu o automatyczne rozpoznawanie twarzy wymaga z reguły zgromadzenia dużych baz danych zawierających zasoby pozwalające na rozpoznanie

[346] A. Tiszbierek, *Komputerowe systemy automatycznej klasyfikacji i rozpoznawania twarzy*, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2013/p111.pdf (dostęp 10.05.2023 r.)

osoby, natomiast weryfikacja tożsamości dokonywana jest często na podstawie wzorca zapisanego w urządzeniu użytkownika (np. telefonie czy komputerze)[347].

W zakresie przykładów wykorzystania omawianej technologii w sferze sektora prywatnego wymienić należy przede wszystkim usługi dostępowe, to jest logowanie do różnego rodzaju urządzeń elektronicznych, w tym telefonów komórkowych, laptopów, tabletów itp. – tzw. face ID. Funkcja ta służy niejako zabezpieczeniu przed dostępem do urządzenia i jego zawartości przez niepożądaną osobę, albowiem przełamanie zabezpieczeń elektronicznych tego rodzaju jest znacznie utrudnione aniżeli w przypadku hasła tradycyjnego. Kolejnym obszarem zastosowania automatycznego rozpoznawania twarzy jest szeroki katalog usług teleinformatycznych, najczęściej spotykanych na portalach społecznościowych, czyli tzw. tagowanie osób widocznych na zdjęciach lub nagraniach wideo. Na tym etapie rozważań zasygnalizować jedynie należy, iż technologia ta wykorzystywana jest również pośrednio w profesji organów ścigania, albowiem wykorzystywana jest m.in. do poszukiwania osób zaginionych, co poddane zostanie badaniu w kolejnej części rozdziału.

3.2. Otworzenie rachunku bankowego metodą na selfie jako przykład wykorzystania sztucznej inteligencji

W przypadku analizy prawnokarnej cyberprzestępstw popełnianych w Polsce, zwłaszcza pod kątem technik wykorzystywanych przez sprawców oraz algorytmów ich ścigania, kilkukrotnie powoływano się na niebezpieczeństwa w cyberprzestrzeni spowodowane umożliwieniem otworzenia rachunku bankowego za pośrednictwem sieci teleinformatycznej. Fakt ten staje się doskonałym narzędziem dla cybersprawców, którzy przy wykorzystaniu tak zorganizowanego środowiska mają możliwość utworzenia rachunków bankowych podszywając się pod inne osoby lub też przy wykorzystaniu tzw. „słupów" a w konsekwencji możliwość transferowania pieniędzy pochodzących z przestępstwa, przez wiele rachunków bankowych.

Możliwość zdalnego utworzenia rachunku bankowego to aktualnie rynkowy standard. Przy okazji omawiania aspektów dotyczących profitów wynikających z zastosowania sztucznej inteligencji, nie sposób pominąć również pewnych zagrożeń wynikających z jej wprowadzenia. Analiza tej kwestii wynika nadto z faktu, iż na kanwie przedmiotowych rozważań, wielokrotnie podejmowano temat dotyczący szeroko rozumianego cyberbezpieczeństwa oraz przestępstw

[347] Szerzej:P. Fajgielski, *Automatyczne rozpoznawanie twarzy – wybrane zagadnienia prawne* [w:] B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), Prawo sztucznej inteligencji i nowych technologii, 2021

popełnianych przy wykorzystaniu sieci teleinformatycznej. Instytucje bankowe, podążając za rozwojem technologicznym oraz chcąc wprowadzić rozwiązania wykorzystujące funkcje sztucznej inteligencji, umożliwiają swoim klientom utworzenie rachunku bankowego na tzw. selfie. Nie pozostawia wątpliwości fakt, iż funkcja ta opiera się wprost na działaniu sztucznej inteligencji, a ściślej mówiąc na automatycznym rozpoznawaniu twarzy jako techniki biometrycznej. Aktualnie możliwość ta jest dostępna m.in. dla klientów Banku Pekao S.A. oraz Millennium S.A., mBank S.A., ING Bank Śląski S.A., Spółdzielcza Grupa Bankowa S.A. a zatem dla najbardziej kluczowych instytucji bankowych oferowanych na polskim rynku.

Instytucje bankowe oferując usługę utworzenia rachunku bankowego sposobem na selfie zapewniają przede wszystkim szybkie, pozbawione formalności zawarcie umowy, na mocy której otwierany jest rachunek bankowy, bez wychodzenia z domu i oczywiście bez opłat. Cały proces ma być błyskawiczny, intuicyjny i przede wszystkim bezpieczny. Banki nie wspominają w treści ofert o wykorzystaniu metod sztucznej inteligencji, sprytnie zasłaniając się pojęciem technik biometrycznych, które przecież w konsekwencji oznaczają w zasadzie to samo. Poważnym wątpliwościom poddać należy jednak bezpieczeństwo zawarcia rzeczonej umowy w ten właśnie sposób. W odniesieniu do procedury utworzenia rachunku bankowego zdalnie wskazać należy, iż we wszystkich instytucjach bankowych proces ten przebiega w zasadzie w ten sam sposób. Pierwszy etap polega na pobraniu aplikacji mobilnej bankowości elektronicznej właściwego banku na urządzenie końcowe oraz utworzeniu konta poprzez wprowadzenie podstawowych danych teleadresowych. Wówczas administrator wyświetla wniosek o utworzenie rachunku bankowego, gdzie wymagane jest podanie danych osobowych, po czym należy wybrać sposób weryfikacji tożsamości. Kolejny krok dotyczy *stricte* weryfikacji tożsamości, przy czym w pierwszej kolejności należy sfotografować rewers i awers dowodu osobistego lub innego dokumentu tożsamości, a następnie – kluczowy z punktu widzenia analizowanych kwestii – krok pt. „zrób sobie selfie". Poza zrobieniem zdjęcia selfie w dobrym oświetleniu, banki wymagają filmu wideo z ruchami głowy – dosłownie kilkusekundowe nagranie, aplikacja kieruje użytkownika w jaki sposób należy to uczynić. W ofertach banki zapewniają o bezpieczeństwie transakcji, obiecując, iż 98% klientów wybierających tę metodę, otwierają konto z sukcesem. W sieci teleinformatycznej nie brakuje filmów instruktażowych wskazujących poszczególne etapy procesu zakładania konta na selfie.

Mając wiedzę na temat etapów procesu otworzenia konta tą metodą, wykorzystującą bez wątpienia komunikację elektroniczną i nowe technologie, możliwe jest płynne przejście do

analizy wykorzystanych w tej procedurze narzędzi opartych na działaniu sztucznej inteligencji. Nie pozostawia w zasadzie wątpliwości fakt, iż procedura weryfikacji tożsamości dokonywana w wyżej opisany sposób wykorzystuje przede wszystkim uczenie maszynowe, techniki biometryczne, a także automatyzację procesu weryfikacji. Uczenie maszynowe to pojęcie w ostatnich latach bardzo spopularyzowane, używane najczęściej w towarzystwie pojęcia sztucznej inteligencji[348]. Często podkreśla się, iż uczenie maszynowe wspiera instytucje finansowe, ale brak jest precyzyjnych informacji o faktycznym sposobie takowego wsparcia. Przyjmuje się, iż uczenie maszynowe automatyzuje budowanie modeli analitycznych poprzez tworzenie algorytmów, które uczą się i dokonują przewidywań na podstawie potężnej liczby danych. Jedną z usług opartą na uczeniu maszynowym, a wykorzystywaną przez instytucje finansowe, w tym bankowe jest właśnie weryfikacja tożsamości. W tym zakresie kluczową rolę odgrywa firma Onfido. Firma Onfido pomaga instytucjom finansowym spełnić wymagania wynikające z zarządzeń i regulacji dotyczących tożsamości klientów przy pomocy uczenia maszynowego. Firma opracowała swoją technologię ML, aby instytucje finansowe mogły w ciągu kilku sekund zweryfikować tożsamość klientów online. Onfido wykorzystuje powszechny dostęp do Internetu, umożliwiając weryfikację tożsamości za pomocą kamery internetowej lub aparatu w smartfonie. Należy zrobić zdjęcie swojego dokumentu tożsamości oraz zdjęcie lub krótkie nagranie swojej twarzy. Następnie technologia uczenia maszynowego firmy Onfido porównuje obraz w dokumencie z cechami biometrycznymi twarzy uchwyconej na zdjęciu i jednocześnie porównuje dokument tożsamości z międzynarodowymi bazami danych kredytowych i listami osób obserwowanych. Reasumując, Onfido to platforma weryfikacji tożsamości oparta na sztucznej inteligencji.

W procesie utworzenia rachunku bankowego po uprzedniej weryfikacji tożsamości za pomocą zdjęcia użytkownika, wykorzystywane są techniki biometryczne, które ściśle dotyczą rozpoznawania twarzy. W celu stworzenia możliwie ogólnej definicji technologii biometrycznych uznać należy, iż są to sposoby identyfikacji oraz weryfikacji tożsamości danej osoby w oparciu o jej cechy indywidualne, w tym m.in. głos, obraz tęczówki oka, linie papilarne, odległość wyznaczonych punktów w strategicznych miejscach twarzy a także geometria dłoni. Weryfikacja w analizowanym przypadku polega na porównaniu danych wygenerowanych przez oprogramowanie na podstawie wizerunku twarzy z wzorcem wykreowanym na podstawie przesłanego zdjęcia dowodu osobistego. Weryfikacja tożsamości

[348] K. Żyłowska, *Czym jest uczenie maszynowe* (Machine Learning), https://aibusiness.pl/czym-jest-uczenie-maszynowe-machine-learning/, (dostęp: 20.05.2023 r.)

polega zatem na potwierdzeniu bądź zaprzeczeniu tożsamości osoby. Narzędzie to przejawia wiele podobieństw względem wyżej przeanalizowanej metody automatycznego rozpoznawania twarzy, przy czym tutaj wykorzystywany jest pewien punkt odniesienia w postaci wygenerowania danych ze zdjęcia dowodu osobistego, zaś w przypadku automatycznego rozpoznawania twarzy weryfikacja tożsamości dokonywana jest często na podstawie wzorca zapisanego w urządzeniu użytkownika (np. telefonie czy komputerze).

Konsekwencja podejmowania tematów nt. nowych technologii, a w tym przypadku sztucznej inteligencji determinuje konieczność postawienia w zasadzie już szablonowego pytania: czy rzeczona transakcja i jej przebieg mają bezpieczny charakter? Brak jest możliwości udzielenia jednoznacznej odpowiedzi w tym zakresie. Rozważania poczynione na tle całości rozprawy wprost wskazują, iż innowacyjne rozwiązania implikują powstanie pewnego zagrożenia, co wprost wynika z niemalże nieograniczonego zasięgu sieci teleinformatycznej, która jak słusznie się wskazuje, jest rajem dla przestępców. Niemniej jednak kompleksowo omówiony sposób utworzenia rachunków bankowych, z prawnokarnego punktu widzenia, dostarcza zdecydowanie więcej pozytywnych aspektów aniżeli ryzyka w cyberprzestrzeni.

W pierwszej kolejności wskazać należy, iż głównym celem wprowadzenia tego rodzaju rozwiązania przez instytucje bankowe było nie tylko maksymalne uproszczenie procedury zawarcia umowy otwarcia rachunku bankowego, ale również zwiększenie dotychczas przyjmowanych zasad bezpieczeństwa wprost dotyczących zdalnego utworzenia konta. Analiza porównawcza dostępnych metod jednoznacznie wskazuje, iż pozostałe metody zdalnego utworzenia konta są zdecydowanie bardziej ryzykowne, aniżeli utworzenie rachunku metodą na selfie, co wynika wprost z jednej przyczyny. Technika biometrycznego rozpoznawania twarzy, oparta o najbardziej możliwie precyzyjnie przygotowane algorytmy sztucznej inteligencji, jest przecież dodatkowym elementem w łańcuchu zabezpieczeń w celu zapewnienia bezpieczeństwa transakcji oraz uniknięcia potencjalnych oszustw w tym zakresie. O ile w przypadku pozostałych metod, potencjalni sprawcy przestępstw mogli wykorzystać dane osobowe innej osoby chociażby poprzez kradzież jej dokumentu tożsamości lub zawartych w nim danych osobowych i teleadresowych, o tyle w przypadku omawianej metody niezbędne jest dodatkowe przejście pozytywnej weryfikacji tożsamości. Mając to na względzie, warunkiem *sine qua non* jest skuteczne i pozytywne porównanie zdjęcia dowodu osobistego lub innego dokumentu ze zdjęciem selfie przesłanym przez wnioskodawcę. Nadto, niektóre

instytucje bankowe, w celu zwiększenia zakresu bezpieczeństwa wymagają przesłania krótkiego filmu, co również ma zapobiec ewentualnym próbom oszustwa.

Niezależnie od powyższego, nie sposób uniknąć przestępczych procederów i w tym zakresie. Wyspecjalizowani (w negatywnym tego słowa znaczeniu) sprawcy nadal usiłują w sposób nielegalny utworzyć w ten sposób rachunki bankowe po to, aby wykorzystać je następczo w przestępczych procederach. Pozytywnie jednak należy ocenić rozwiązania wprowadzone przez banki, albowiem postępowań karnych związanych bezpośrednio z tą metodą, jest zdecydowanie mniej aniżeli dotychczas uznawany za tradycyjny, zdalny model utworzenia rachunku bankowego. Co więcej, przypadki te dotyczą co do zasady prób przestępczego działania (usiłowania), nie zaś faktycznego jego dokonania. Z prawnokarnego punktu widzenia, zasygnalizować jedynie należy, iż wówczas postępowania takie prowadzone są w zakresie przestępstwa spenalizowanego w art. 190a § 2 kodeksu karnego, to jest wykorzystania cudzych danych osobowych w celu wyrządzenia mu szkody majątkowej lub osobistej. Postępowania karne inicjowane są co do zasady zawiadomieniami instytucji bankowych, które ujawniają transakcje, w których algorytmy sztucznej inteligencji negatywnie zweryfikowały tożsamość wnioskodawcy i ustalano, iż osoba podająca dane osobowe oraz zdjęcie dokumentu tożsamości, po przesłaniu zdjęcia i nagrania wideo z wizerunkiem twarzy, nie wykazuje zgodności z przesłanymi danymi. Każda z prób utworzenia rachunku bankowego w ten sposób, analogicznie jak w poprzednio omawianych metodach zdalnego utworzenia rachunku bankowego jest rejestrowana przez instytucje bankowe, co umożliwia organom ścigania pozyskania m.in. numeru IP wykorzystanego przez sprawcę, a co więcej – zdjęcia zawierającego wizerunek sprawcy, co ułatwia ustalenie jego tożsamości, a w konsekwencji pociągnięcia do odpowiedzialności karnej.

Nadmienić bez wątpienia należy, iż gwarantowany przez banki bezpieczny charakter przeprowadzanej transakcji to jest utworzenie w omawiany sposób rachunku bankowego, w rzeczywistości wcale nie jest tak doskonałym rozwiązaniem jak mogłoby się wydawać. Wątpliwości budzi bowiem fakt czy biometria to faktycznie aż tak bezpieczna forma uwierzytelniania[349]. Na kanwie przedmiotowej pracy wielokrotnie wskazywano, iż w przypadku procesu wykrywczego podejmowanego przez organy ścigania niezbędne jest

[349] Szerzej: D. Dajnowicz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E.W. Pływaczewski (red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku*, 2022

dopasowanie schematu i metod działania do modelu przestępczego zachowania sprawcy. Zatem wykrycie sprawcy działającego w sieci teleinformatycznej, wymaga lustrzanego działania ze strony organów ścigania. Mając na względzie tę konkluzję, należałoby postawić otwarte pytanie: czy sztuczna inteligencja może stanowić zagrożenie dla siebie samej? Co więcej, czy systemy oparte na działaniu algorytmów sztucznej inteligencji mogą zostać wprowadzone w błąd przez tożsame modele działania? W Polsce mechanizmy dotyczące sztucznej inteligencji są na bardzo wczesnym stadium zaawansowania. Zaryzykować można nawet stwierdzeniem, iż jest ona nie do końca poznana, zwłaszcza z perspektywy organów ścigania i wymiaru sprawiedliwości. Niezależnie od powyższego, wskazać jednak należy, iż sztuczna inteligencja wyposażona jest w zdolność odtworzenia wizerunku konkretnej osoby nawet po analizie 30 sekundowego nagrania wideo, przy czym – co zaskakujące – odtwarza wizerunek danej osoby z niezwykłą precyzją i doskonałością, w sposób, który (nawet przy wykorzystaniu czynnika ludzkiego, nie maszynowego) jest niemalże niemożliwy do odróżnienia z rzeczywistym wizerunkiem danego człowieka.

W związku z powyższym, fakt ten nie staje się niejako możliwością dla potencjalnych sprawców, którzy za pomocą ogólnodostępnych programów, mogą odtworzyć czyjś wizerunek, bez jego wiedzy, a następnie wykorzystać go dla utworzenia rachunku bankowego metodą na selfie. Skoro człowiek nie jest w zasadzie w stanie w większości przypadku dostrzec różnicy i wykryć ewentualnej rozbieżności, to czy oprogramowanie oparte na działaniu sztucznej inteligencji i nowych technologii jest w stanie skutecznie poradzić sobie z tym zadaniem? Praktyka wprost wskazuje, iż jedyna słuszna odpowiedź na postawione wyżej pytanie to odpowiedź bez wątpienia pozytywna.

4. Potencjał sztucznej inteligencji wśród zawodów korporacyjnych

Specyfika zawodów prawniczych sprawia, iż trudno sobie wyobrazić sytuację, w której narzędzia oparte na działaniu schematów sztucznej inteligencji mogłyby zastąpić profesję wykonywaną przez zawody prawnicze. Przemawia za tym wiele istotnych czynników, w tym zwłaszcza fakt, iż nauki prawnicze należą bez wątpienia do katalogu nauk społecznych, zaś każdorazowa sprawa podejmowana przez prawników wymaga dogłębnej, szczegółowej analizy dokonanej przez człowieka, a ściślej przez profesjonalnego prawnika przy wykorzystaniu zasad rozumowania w powiązaniu z przekonaniami rozumianymi jako zasady doświadczenia życiowego. Mogłoby się wydawać, iż poszczególne sprawy wykazują się dużym podobieństwem, niemniej jednak szczegółowa analiza bezpośrednio wskaże na pewne niuanse

i czynniki, które nie tylko będą różnicą, ale będą czynnikiem determinującym podjęcie określonych decyzji prawnych i prawniczych. W poprzedniej dekadzie w zasadzie niewyobrażalne było, aby sztuczna inteligencja chociażby w najmniejszym stopniu mogła zastąpić zawody prawnicze. Prawnicy zatem byli spokojni o swój los, wykazując głębokie przekonanie, iż ich byt na rynku jest bezpieczny i niezagrożony przez jakiekolwiek maszyny wykorzystujące potencjał nowych technologii. Nieustannie rosnąca popularność nowych technologii, budzący podziw postęp technologiczny oraz docieranie sztucznej inteligencji do najmniej spodziewanych sektorów gospodarki, sukcesywnie, na przestrzeni lat osłabiał rzeczone poczucie bezpieczeństwa tej profesji, powodując liczne dywagacje oraz wątpliwości co do sensu bytu prawników w przyszłości. Fakt powtarzalności konstruowanych umów, możliwość sformułowania pewnych postanowień według precyzyjnie opracowanego wzorca niejako stworzył w tym zakresie możliwości dla sztucznej inteligencji, aby rozszerzyć jej działalność również w sektorze zawodów prawniczych.

Poniżej analizie poddane zostaną możliwości zastosowania szeroko rozumianej sztucznej inteligencji wśród zawodów prawniczych, zwłaszcza w kontekście ich praktycznego wykorzystania oraz rzeczywistej przydatności w codziennym funkcjonowaniu różnych grup zawodowych. Ostatecznie podjęta zostanie próba oceny faktycznego sensu wprowadzenia tych narzędzi do branży prawniczej oraz przede wszystkim próba oszacowania stopnia zagrożenia dla funkcjonowania zawodów prawniczych. Nadto badaniu podlegać będzie kwestia dotychczas wykorzystywanych narzędzi opartych o funkcjonowanie nowych technologii, poziomu ich zaawansowania.

W pierwszej kolejności zastanowić należy się nad tym, w jakiej konkretnie sferze związanej z branżą prawniczą sztuczna inteligencja faktycznie mogłaby przynieść pożądany rezultat i co w rzeczywistości jest tym najbardziej oczekiwanym czynnikiem. Nie pozostawia w zasadzie wątpliwości fakt, iż głównym czynnikiem determinującym chęć skorzystania z innowacyjnych metod związanych z oprogramowaniem sztucznej inteligencji jest kwestia czasu i możliwe maksymalne jego „zaoszczędzenie", co w konsekwencji przekłada się na wiele innych okoliczności, w tym zwłaszcza kwestie ekonomiczne i finansowe *stricte* związane z możliwością pozyskania większych zarobków. W zależności od konkretnych zawodów prawniczych, nieco inaczej przedstawiają się możliwości odnośnie skorzystania z potencjału sztucznej inteligencji, albowiem większe szanse w tym zakresie oferują wolne zawody, zwłaszcza działalność radców prawnych i adwokatów, a w konsekwencji bardziej ograniczona jest ta sfera w przypadku działalności organów ścigania i wymiaru sprawiedliwości. W celu

możliwie rzetelnego i zupełnego przeprowadzenia badań w tym zakresie, wynikiem których będzie oszacowanie stopnia zagrożenia bytu zawodów prawniczych przez zastąpienie ich sztuczną inteligencją, w pełni celowe i uzasadnione jest omówienie aspektów związanych ze sztuczną inteligencją w odniesieniu do konkretnych grup zawodowych. Tylko taka analiza pozwoli na zobrazowanie faktycznego zagrożenia zawodów prawniczych, a także wyprowadzenia wniosków, który zawód prawniczy potencjalnie jest najbardziej zagrożony.

W związku z tym, iż specyfika zawodów korporacyjnych pozwala na stwierdzenie, iż jest to środowisko mające największy potencjał w zakresie skorzystania z możliwości sztucznej inteligencji, a także środowisko, w którym rywalizacja i konkurencja na rynku osiąga zaawansowany poziom, od tej branży należy rozpocząć rozważania w tym zakresie. Jedynie zasygnalizować bardzo ogólnie należy, iż praca tej grupy zawodowej dotyczy bardzo szerokiego katalogu czynności, wśród których wyodrębnić należy tzw. kwestie organizacji pracy, kontakt z klientami, analiza materiałów, analiza przepisów prawnych, sporządzanie pism procesowych i umów oraz występowanie w charakterze pełnomocnika przez sądami, względnie innymi instytucjami, w tym organami wymiaru sprawiedliwości. Ewentualne wykorzystanie potencjału sztucznej inteligencji w ramach świadczenia usług przez wolne zawody odbywać się może przede wszystkim na płaszczyźnie zautomatyzowania konkretnych czynności, a tym samym przyspieszenia pewnych procesów, z pozostawieniem udzielania porad prawnych w zasadzie na tożsamym jak dotychczas obowiązujący modelu funkcjonowania[350].

Sfera budząca wśród prawników największą obawę o ich byt dotyczy bezpośrednio merytorycznej płaszczyzny ich pracy oraz funkcjonowania na rynku i odnosi się wprost do udzielania porad prawnych, które bezapelacyjnie stanowią fundament pracy adwokata i radcy prawnego. Nie pozostawia wątpliwości fakt, iż sztuczna inteligencja może polepszyć funkcjonowanie wielu kancelarii prawnych i dla wielu profesjonalistów zdaje się być szansą na gratyfikację prowadzonych przez nich działalności gospodarczych. Niemniej jednak obawa przed potencjalnym zastąpieniem tej grupy zawodowej przez uczenie maszynowe i urządzenia wykorzystujące działanie sztucznej inteligencji, zdecydowanie jest przeważającym odczuciem, przez pryzmat którego ocenia się rozwój sztucznej inteligencji i coraz szersze jej zastosowanie w branży prawniczej.

[350] Szerzej: R. Koch., *Legal Tech i nowoczesne technologie w pracy prawników wewnętrznych* [w:] K. Dzioba (red.), R. Rybicki (red.), Metodyka pracy prawnika in-house, 2021

Ewentualne możliwości faktycznego zastosowania sztucznej inteligencji w zawodach korporacyjnych, aby rzeczywiście odniosły istotny wpływ na byt tej branży zawodowej, jak wyżej wskazano, dotyczą bezpośrednio kwestii udzielania porad prawnych, zatem to w tym aspekcie należy ulokować wszelkie rozważania w tym zakresie. Wcale nie wybitnie innowacyjnym oraz nie niemożliwym do spełnienia rozwiązaniem, które można zauważyć np. w niektórych stanach USA, ale nie tylko, jest wprowadzenie chatboxów opartych o algorytmy sztucznej inteligencji. Jak sama nazwa wskazuje, jest to forma chatu, a zatem komunikacji prowadzonej na odległość, przy wykorzystaniu środków komunikacji elektronicznej, przy czym po jednej ze stronie znajduje się tzw. „algorytmiczny prawnik", a ściślej wskazując, sztuczna inteligencja, która po analizie nadesłanych informacji od potencjalnego klienta jest w stanie odpowiednio zakwalifikować do konkretnej kategorii daną sprawę, a następnie po przeprowadzeniu analizy „wgranego" w oprogramowanie orzecznictwa i przepisów, wyda rozstrzygnięcie prawne. Skuteczność takiego rozwiązania możliwa byłaby do ocenienia dopiero po jej rzeczywistym funkcjonowaniu przez określony czas, niemniej jednak można spekulować nad prawdopodobnymi wynikami i wyprowadzić, być może przedwczesne wnioski, które poruszone zostaną przy okazji szacowania ryzyka zastąpienia zawodów prawniczych przez sztuczną inteligencję.

Nie ma możliwości dokładnej oceny wpływu szeroko rozumianych nowych technologii na funkcjonowanie zawodów prawniczych, dlatego też, poza narzędziami wzbudzającymi poczucie zagrożenia wśród prawników, celowe jest wskazanie na możliwości zastosowania potencjału sztucznej inteligencji, która nie tylko ułatwi, ale również udoskonali działalność profesji prawniczej. Kwestia ta dotyczy bezpośrednio modelu, którego nazewnictwo może sprowadzać się do stwierdzenia, iż są to narzędzia analizy predykcyjnej, które mogłyby prawnikom pomoc wybrać najkorzystniejszą strategię działania[351] m.in. na sali rozpraw, przy jednoczesnym zminimalizowaniu poświęconego w tym zakresie czasu. Analiza obszernej dokumentacji dostarczonej przez klienta pochłania zdecydowaną część czasu prawników w odniesieniu do finalnego efektu w postaci udzielenia porady prawnej w ostatecznym jej kształcie[352]. Rzeczone narzędzie w sposób zdecydowany pozwoliłoby na skrócenie czynnika czasu, albowiem system przygotowywałby nie tylko projekty strategii, ale również wyszczególniałby najważniejsze fakty i dane z wprowadzonej dokumentacji. Model taki z pewnością znalazłby również zastosowanie w toku prowadzonych negocjacji z klientem

[351] Np. Case Cruncher Alpha w Londynie

[352] R. Koch, *Legal Tech i nowoczesne technologie w pracy prawników wewnętrznych* [w:] K. Dzioba (red.), R. Rybicki (red.), Metodyka pracy prawnika in-house, 2021

i ewentualnie stroną przeciwną. Z uwagi na wprowadzenie do tego systemu danych szczególnie wrażliwych, bez wątpienia oprogramowanie takie musiałoby spełniać wszelkie certyfikaty bezpieczeństwa pozwalające na zapewnienie skutecznej ochrony danych osobowych zgodnie z obowiązującymi przepisami. Niezależnie od powyższego w kwestii możliwości wprowadzenia tak innowacyjnych rozwiązań, nie sposób pominąć kwestii związanych z podstawową zasadą bezpieczeństwa obrotu gospodarczego, której gwarantem są najogólniej ujmując prawnicy, do których społeczeństwo ma zaufanie zwłaszcza w zakresie zgodności z prawem realizowanych czynności.

Poza wyżej zasygnalizowanymi sferami działalności branży wolnych zawodów, nie sposób zapomnieć o kolejnym kluczowym i niekiedy wiodącym aspekcie pracy tej grupy zawodowej, czyli o konstruowaniu umów różnego rodzaju[353]. Jak wskazywano na tle rozważań podejmowanych w poprzednich rozdziałach, przedmiotem działalności prawników jest również formułowanie postanowień umów, w tym niejednokrotnie o bardzo skomplikowanym charakterze umów spółek, czy też innych umów zawieranych między podmiotami gospodarczymi. Algorytmy sztucznej inteligencji, uczenia maszynowego na tej płaszczyźnie również mogłyby dostarczyć satysfakcjonujących wyników w przypadku stworzenia systemu i oprogramowania stanowiącego pomoc w konstruowaniu umów tego rodzaju. Potencjał sztucznej inteligencji, oceniany przez pryzmat dotychczasowych możliwości, mógłby przygotowywać propozycje postanowień umownych zgodnych z powszechnie obowiązującym prawem, co po uprzedniej weryfikacji akceptowane byłoby przez profesjonalny podmiot. Narzędzie takie dostarczałoby możliwości skonstruowania w zasadzie całokształtu konkretnego rodzaju umowy na podstawie uczenia maszynowego, oczywiście po uprzednim wprowadzeniu niezbędnych danych, w tym rodzaju umowy. Co więcej, rzeczone narzędzie umożliwiałoby nie tylko pracę nad konstruowaniem umowy, ale także pracę nad już sformułowanym i przekazanym do analizy i oceny aktem poprzez ewentualne ujawnienie postanowień zawierających klauzule abuzywne czy postanowienia niezgodne z prawem. Prognozować można, iż takie narzędzie w sposób znaczny polepszyłoby komfort pracy zwłaszcza radców prawnych, którzy w zdecydowanej większości zajmują się sprawami o charakterze gospodarczym. Wskazać należy, iż co prawda funkcjonuje narzędzie opierające się o wyżej wspomniany sposób działania, to jest chat GPT, niemniej jednak praktyka wskazuje, iż nie jest on stosowany wśród zawodów prawniczych, co wynika przede wszystkim z nie do

[353] Szerzej: P. Księżak, *Zawieranie umów przez sztuczną inteligencję* [w:] M. Dumkiewicz (red.), K. Kopaczyńska-Pieczniak (red.), Szczotka Jerzy (red.), Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie. Tom II, 2020, i

końca zweryfikowanego charakteru tego urządzenia, jak również wątpliwości jakie pojawiają się w związku z ewentualną ochroną praw autorskich w związku z tym. Zasygnalizować jedynie należy, iż Chat GPT (*Generative Pre-trained Transformer*) jest to model językowy oparty o działanie sztucznej inteligencji, który służy do generowania tekst w sposób naturalny i spójny, wykorzystuje architekturę GPT-4 do analizy danych tekstowych, tworzenia odpowiedzi na pytania i prowadzenia płynnych, interaktywnych rozmów z użytkownikami[354].

5. Sztuczna inteligencja wśród organów ścigania i wymiaru sprawiedliwości

W związku z tym, iż sfera działalności zarówno organów ścigania jak i wymiaru sprawiedliwości odnosi się do zagadnień dotyczących sektora publicznego, a także zakresu spraw bezpośrednio dotyczących obywatela, kategorycznie stwierdzić należy, iż nie jest to miejsce przeznaczone do wprowadzenia eksperymentalnych rozwiązań, w tym opartych o funkcjonowanie sztucznej inteligencji. Praktyka w zasadzie bezlitośnie wskazuje, iż wśród organów ścigania dostrzega się wyłącznie sprawdzone, przetestowane, bezpieczne, zwłaszcza pod względem prawnym narzędzia, co do których nie ma absolutnie żadnego ryzyka zarówno błędu, nieuprawnionego dostępu do danych jak również ewentualnego wyrządzenia jakiejkolwiek szkody. Stąd też możliwość zastosowania algorytmów sztucznej inteligencji w tym zakresie, analizowana może być w zasadzie wyłącznie w sferze hipotetyzowania i niejako pozytywnego patrzenia w przyszłość przez pryzmat dopuszczenia do tej branży większej ilości innowacyjnych rozwiązań, co z pewnością przyczyniłoby się do zwiększenia efektywności prowadzonych i nadzorowanych postępowań karnych.

Nie ma wątpliwości co do tego, iż rozwiązania wykorzystujące potencjał sztucznej inteligencji są jak najbardziej potrzebne wśród wszystkich branży prawniczych, a zwłaszcza wśród organów ścigania. Fakt ten bezpośrednio determinuje nieustannie rosnąca liczba cyberprzestępstw popełnianych na terenie kraju, a w konsekwencji potrzeba właściwego reagowania organów ścigania i dostosowywania algorytmów ścigania cybersprawców. Potrzeba wprowadzenia poniżej przedstawionych rozwiązań wynika wprost z praktyki oraz przebiegu procesu wykrywczego organów ścigania i podyktowana jest przede wszystkim koniecznością przyspieszenia postępowań karnych, a w konsekwencji większą szansą na wykrycie sprawców przestępstw.

[354] https://obtk.pl/slownik/chat-gpt-co-to-jest/ (dostęp: 30.05.2023 r.)

Jak podkreślano na kanwie poprzednich rozdziałów, nie ma podstaw do uznania, iż informatyzacja organów ścigania znajduje się na możliwie najniższym poziomie, albowiem fakt ten byłby niezgodny z rzeczywistością. Sfera ta próbuje nadążyć nad nieustannie prosperującym rozwojem technologicznym wprowadzając szereg rozwiązań, które dokładnie przeanalizowano we wstępnej części przedmiotowej pracy. Wśród rozwiązań, które z kolei mogą w przyszłości potencjalnie umożliwić wprowadzenie szeregu bardziej zaawansowanych narzędzi, w tym opartych o sztuczną inteligencję, jest możliwość digitalizacji akt postępowań karnych. Fakt przechowywania materiałów postępowania przygotowawczego w formie zdigitalizowanej, czyli elektronicznej umożliwia nie tylko ich udostępnienie na odległość stronom postępowania, ale również dostarcza możliwości ich analizy w zdecydowanie przyspieszonym tempie.

W przypadku cyberprzestępstw, w przypadku których możliwe jest opracowanie ogólnego algorytmu dotyczącego procesu wykrywczego, oczywiście odpowiednio dostosowanego do konkretnego stanu faktycznego, zastosowanie narzędzi opartych o działanie sztucznej inteligencji mogłoby przynieść nieprawdopodobnie satysfakcjonujące rezultaty. Oparty o system uczenia maszynowego program, na podstawie analizy zdigitalizowanych materiałów postępowania przygotowawczego, mógłby wyselekcjonować dane, co do których zachodzi konieczność ich procesowego zabezpieczenia, jednocześnie ustalając rejestracje procesowe danej zmiennej, np. numeru rachunku bankowego, numeru telefonu czy innych danych retencyjnych. Narzędzie takie pozwoliłoby przede wszystkim na przyspieszenie postępowania przygotowawczego jeszcze na przedpolu dochodzenia lub śledztwa, zminimalizowanie czynnika czasu poprzez uniknięcie konieczności analizy całych akt sprawy, a także uniknięcie ryzyka ewentualnego pominięcia pewnych danych, które mogłyby pozwolić na ustalenie tożsamości sprawcy. Nadto ustalenie rejestracji procesowych danej zmiennej, to jest sprawdzenie czy inna jednostka prokuratury prowadziła lub prowadzi postępowanie przygotowawcze w zakresie przestępstwa, w którym ją wykorzystano, pozwoliłaby na uniknięcie jednoczesnego prowadzenia postępowań o tożsamym zakresie podmiotowym i przedmiotowym, a także ustalenie powiązań i zależności między już toczącymi się postępowaniami przygotowawczymi. Postępowania przygotowawcze nadzorowane przez kilka jednostek, a w zasadzie o tożsamym modus operandi, przy wykorzystaniu tych samych metod działania przez sprawców i tych samych danych retencyjnych, mogłyby być sprawniej łączone do wspólnego wprowadzenia zgodnie z zasadami przyjętymi w Rozporządzeniu Ministra Sprawiedliwości z dnia 7 kwietnia 2016 roku Regulamin wewnętrznego urzędowania

powszechnych jednostek organizacyjnych prokuratury[355]. Niemniej jednak dla precyzji, niezbędny do odnotowania jest fakt, iż każdorazowo wyżej opisane działania, pomimo analizy która miałaby być dokonywana przez przeznaczone ku temu oprogramowania i systemy, weryfikowane musiałyby być przy wykorzystaniu czynnika ludzkiego, aby zapobiec ewentualnym pomyłkom.

Całokształt przywołanych okoliczności wprost wskazuje, że sztuczna inteligencja bezpośrednio może wpłynąć na statystykę w zakresie wykrywalności przestępstw, zwłaszcza popełnianych za pośrednictwem sieci teleinformatycznej, a także na kwestię przewidywalności cyberataków[356], a w konsekwencji bezapelacyjnie wpłynąć na walkę z cyberprzestępczością oraz zwiększyć efektywność prowadzonych postępowań karnych w tym zakresie[357]. Nadmienić należy, iż sztucznej inteligencji nie należy ignorować, jest to bowiem mechanizm, który na skutek rozwoju technologicznego, może zostać wykorzystany przez cyberprzestępców na bardzo szeroką skalę. W środowisku prawniczym słusznie się wskazuje, iż ww. sprawcy mają w ten sposób możliwość niejako zautomatyzowania swoich ataków.

Wyżej poczynione rozważania, nie pozostawiają wątpliwości, iż udostępnienie wśród organów ścigania bardziej zaawansowanych i innowacyjnych narzędzi opartych o działanie sztucznej inteligencji, przyniosłoby szereg pozytywnych skutków. Poza wyżej opisaną możliwością, niezwykle pożądanym rozwiązaniem jest wprowadzenie systemu opartego o działanie sztucznej inteligencji, który analizowałby obszerne zbiory bazy danych. W takim modelu wyróżnić można kilka aspektów, wśród których takie rozwiązanie byłoby niezwykle przydatne. Poza analizą danych retencyjnych, za pomocą których można zidentyfikować i ustalić tożsamość sprawców przestępstw, a zatem sferą ściśle związaną z procesem wykrywczym prowadzonym w toku postępowania przygotowawczego, istnieją również inne obszary, które niejako potrzebują wsparcia innowacyjnych technologii. Jednym z rzeczonych sfer jest tzw. profilowanie, w tym profilowanie sprawców przestępstw[358]. Profilowanie to zautomatyzowana metoda eksploracji danych, która polega na ich konwersji w indywidualne

[355] Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 roku Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz. U. 2016 poz. 508)
[356] M. Skolimowski, *Polityka cyberbezpieczeństwa w świetle zagrożenia cyberterroryzmem*, [w:] G. Szpor (red.), A. Gryszczyńska (red*.) Internet. Strategie bezpieczeństwa*, Warszawa 2017, s. 107
[357] Szerzej: D. Dajnowicz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E. W. Pływaczewski (red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku*, 2022
[358] Szerzej: K. Mamak, Rewolucja cyfrowa a prawo karne, Krakowski Instytut Prawa Karnego Fundacja, 2019 oraz M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Wolters Kluwer, 2020

lub grupowe profile[359]. Przyjmuje się, iż to automatyczny proces szukania prawidłowości w zbiorach danych w celu tworzenia profili służących do analizowania preferencji i przewidywania zachowań, a czasem również podejmowania decyzji, w tym automatycznych[360]. Warto zaznaczyć, iż algorytmy sztucznej inteligencji wykorzystywane są już w ten sposób na świecie[361], gdzie doskonale się sprawdzają. System taki funkcjonuje m.in. w USA, gdzie na podstawie narzędzia Compas (*Correctional Offender Management Profiling for Alternative Sanctions*) oceniana jest predyspozycja powrotu do przestępstwa przez skazanego[362] i na tej podstawie analizowana jest możliwość warunkowego przedterminowego zwolnienia z odbywania pozostałej części kary pozbawienia wolności[363].

AI w procesie profilowania sprawców przestępstw, na różnym etapie zaawansowania postępowania karnego, począwszy od postępowania przygotowawczego aż do postępowania wykonawczego, przyniosłoby rezultaty, które być może bez tego wsparcia są niemożliwe do osiągnięcia. W zakresie profilowania sprawców, oprogramowania sztucznej inteligencji wspierałyby organy ścigania w zakresie zdolności do przewidywania ponownego popełnienia przestępstwa czy też zorganizowania konkretnych ataków na danym obszarze[364]. Fakt ten z kolei pozwoliłyby, chociażby w jakiejkolwiek części, zminimalizować ilość przestępstw i zapobiec ich popełnianiu, co jest przecież naczelną zasadą procesu karnego. Omawiając kwestię analizy obszernych zbiorów baz danych, nie sposób nie wspomnieć o niezbędnym wsparciu w zakresie pozyskiwania danych z takich katalogów, chociażby w zakresie pobieranych odcisków daktyloskopijnych od osób podejrzanych. Do około 2010 roku procedura pobierania daktyloskopii od podejrzanych przebiegała w następujący sposób. Odciski palców pobierane były na tzw. dokument, po czym były skanowane, a dopiero wówczas wprowadzane do systemu komputerowego. Postęp technologiczny szczęśliwie wymusił wprowadzenie zmian w tym zakresie, na skutek czego zaczęto wykorzystywać w tym celu tzw. life scaner, czyli urządzenie, dzięki któremu wystarczającym jest umieszczenie palca na płytce, która bezpośrednio odczytuje linie papilarne, a za pomocą czytnika elektronicznej informacja od razu trafia do centralnej bazy danych. Skoro jednostki policji wyposażone są w

[359] M. Kusak, T. Pawłowski, *Zawody prawnicze a sztuczna inteligencja*, Rynek Pracy 2020, s. 38-39
[360] Hildebrandt 2006, s. 548– 552; Bosco i in. 2015, s. 3–33
[361] Szerzej: Calo R., *Robots in American Law*, „Legal Studies Research Paper" 2016/4
[362] wyrok Sądu Najwyższego Stanu Wisconsin z 13 lipca 2016 r. w sprawie State przeciwko Loomis, sygn. 881 N.W.2d 749 (2016)
[363] Szerzej: F. Rahman, COMPAS Case Study: Fairness of a Machine Learning Model, "Towards Data Science", 7 września 2020 r.
[364] Lightbourne J., *Damned Lies & Criminal Sentencing using evidence-based tools*, 15 *D*uke *L*aw *&* *T*echnology R*eview*, 2017, s. 330-333

urządzenie niejako automatycznie przekazujące informacje do zbioru bazy danych, przydatne byłoby zaprojektowanie oprogramowania opartego o działanie sztucznej inteligencji, które pozwoliłoby na automatyczną analizę obszernych baz danych oraz wyprowadzenie pożądanych wniosków, np. w zakresie uprzedniej rejestracji procesowej danej osoby. Analogiczne rezultaty pożądane są również w przypadku procedury ustalenia tożsamości osoby zmarłej, pobranie od takiej osoby profilu genetycznego lub odcisków palców mogłoby przyspieszyć zidentyfikowanie zmarłego, a w konsekwencji ustalenie kręgu osób dla niego najbliższych. Z uwagi na coraz to szersze wykorzystanie sztucznej inteligencji w zakresie automatycznego rozpoznawania twarzy oraz generalnie kwestii związanych z odtwarzaniem obrazu, rozważyć należy również potencjał wykorzystania tej technologii w zakresie zagadnień kryminalistycznych, a ściślej wskazując w procesie odtwarzania wizerunku sprawcy i sporządzania portretów pamięciowych. Nie budzi wątpliwości fakt, iż aspekt sporządzania portretów pamięciowych wśród technik kryminalistycznych jest bardzo istotnym elementem, przyczyniającym się w ogromnym stopniu do wykrycia sprawcy przestępstwa. Omawiane narzędzie po wprowadzeniu szkicu sporządzonego przez rysownika, przy wykorzystaniu uczenia maszynowego, umożliwiałoby sporządzenie portretu sprawcy, po uprzednim wprowadzeniu do systemu szczegółowych danych w postaci chociażby cech charakterystycznych. Co więcej, przy przyjęciu, iż system odtwarzałby wizerunek w czasie rzeczywistym, możliwe byłoby modyfikowanie portretu i natychmiastowe okazywanie go np. pokrzywdzonemu czy potencjalnemu świadkowi kryminalnego zdarzenia. Wspomnieć należy, iż na początku 2023 roku pojawił się na rynku projekt programu o nazwie Forensic Sketch AI-rtist[365], który w założeniu ma tworzyć bardzo realistyczne policyjne szkice podejrzanego na podstawie danych wprowadzonych przez użytkownika, niemniej jednak na stwierdzenie jego sukcesu lub niepowodzenia potrzeba znacznego upływu czasu, o ile jego funkcjonowanie w kryminalistyki w ogóle się przyjmie. Powtórzyć należy, iż za celowością wprowadzenia tego typu rozwiązań przemawia przede wszystkim fakt, iż portrety stworzone przez sztuczną inteligencję są tak realistyczne i doskonale przygotowane, że są nie do odróżnienia od prawdziwego zdjęcia. Fakt ten potwierdza m.in. eksperyment przeprowadzony przez zespół amerykańskich psychologów pod przewodnictwem Sophie J. Nightingale i Hany'ego Farida[366], w ramach którego w pierwszej fazie 315 badanych osób oceniało prawdziwość 128 zdjęć. Prawidłowo wskazano prawdziwe zdjęcie jedynie w 48,2 procent przypadków.

[365] Program. Artur Furtanato i Filipe Reynaud
[366] https://www.pnas.org/doi/10.1073/pnas.2120481119 (dostęp: 02.06.2023 r.)

Poza wyżej kompleksowo omówionymi narzędziami wykorzystującymi w znacznej części uczenie maszynowe sztucznej inteligencji, a które mogłyby odnieść satysfakcjonujące wyniki w pracy organów ścigania, w pełni celowe i uzasadnione jest poruszenie kwestii potrzeby stworzenia oprogramowania wspierającego pracę organów ścigania na wielu płaszczyznach, głównie w zakresie podejmowania decyzji o charakterze procesowym. Praktyka wprost wskazuje, iż zdecydowana większość spraw inicjujących postępowanie karne ma charakter powtarzalny, nieskomplikowany, o bardzo przewidywalnym i możliwym do odtworzenia przebiegu. Zastosowanie oprogramowania, które wesprze organy ścigania sformułowaniem projektu decyzji procesowej w postaci wszczęcia postępowania przygotowawczego albo odmowy wszczęcia, w sposób znaczny skróciłoby czas procedowania w tego rodzaju sprawach, pozostawiając jednocześnie więcej czasu i uwagi na sprawy o bardziej zaawansowanym skomplikowaniu. Oczywiście wątpliwości budzić może trafność podejmowanych decyzji przez sztuczną inteligencję, niemniej jednak po raz kolejny wskazać należy, iż rozwiązania takie miałyby wyłącznie charakter pomocniczy, a nie zasadniczy. Nadto w praktyce organów ścigania, wielokrotnie pojawiają się wątpliwości i dylematy przede wszystkim na płaszczyźnie konieczności zastosowania środków zapobiegawczych oraz ich rodzaju, nie tylko w celu zapewnienia prawidłowego toku postępowania przygotowawczego, ale również w celu zapewnienia maksymalnej ochrony i bezpieczeństwa pokrzywdzonych oraz potencjalnych pokrzywdzonych. Model oprogramowania, do którego wprowadzano by kluczowe dane, przy wykorzystaniu algorytmów sztucznej inteligencji, proponowałby organom ścigania zastosowanie konkretnego środka zapobiegawczego – czy to o charakterze izolacyjnym, czy też wystarczające będzie przyjęcie wolnościowych środków. System oparty o uczenie maszynowe, prognozowałby m.in. możliwość ponownego popełnienia przestępstwa, profilowałby podejrzanego, szacował ryzyko i współczynnik wpływu na prawidłowy tok postępowania, a także charakter czynności niezbędnych to wykonania, co do których podejrzany mógłby podejmować czynności utrudniające ich przebieg. Kolejno wskazać należy na wyłącznie wspierający charakter takiego instrumentu, pozwalający na zniwelowanie czasu potrzebnego do analizy i podjęcia właściwej decyzji, a ostateczna jej formuła, przy przyjęciu nawet najbardziej doskonałego oprogramowania, powinna zostać zweryfikowana przez prokuratora. Wyłącznie taka konstrukcja zapewni możliwość osiągnięcia celów postępowania, z zachowaniem podstawowych zasad postępowania karnego, przy jednoczesnym poszanowaniu praw i obowiązków podejrzanego, bez uprzedniego nastawienia do konkretnej osoby.

Prawo i nowe technologie oraz sztuczna inteligencja to nie tylko właściwe na tej płaszczyźnie regulacje prawne, ale również możliwość praktycznego wykorzystania potencjału sztucznej inteligencji i rozwiązań innowacyjnych, również przez wymiar sprawiedliwości. Wydawać by się mogło, iż ta profesja zdaje się być najmniej zagrożona zastąpieniem przez sztuczną inteligencję, albowiem najtrudniej wyobrazić sobie narzędzia wykorzystujące jej algorytmy w pracy sędziego[367]. Niemniej jednak, postulat maksymalnego przyspieszenia i ułatwienia wszelkich możliwych formalności, bezpośrednio pociąga za sobą potrzebę zautomatyzowania pewnych czynności procesowych, właśnie przy wykorzystaniu uczenia maszynowego. Analiza funkcjonowania rynku prawniczego, a zwłaszcza branży wymiaru sprawiedliwości wymusza jednakże ostudzenie emocji w tym zakresie oraz niewybieganie za bardzo w przyszłość, aczkolwiek futurologicznie rozważyć można pewne kwestie. W pierwszej kolejności jednoznacznie podkreślić należy, iż wszelkie omówione poniżej narzędzia ocenić należy wyłącznie z perspektywy narzędzi wspomagających pracę sędziów. Aby móc go z czystym sumieniem wdrożyć w tak wrażliwym obszarze, jak wymiar sprawiedliwości, musimy mieć pewność, że jego działanie wiąże się z rzeczywistą wartością dodaną, a zarazem nie niesie ze sobą efektów ubocznych, jak np. dyskryminacja[368]. Pamiętać nadto należy, iż kryterium ekonomiki procesowej nie może być jednym i dominującym, zwłaszcza w przypadku organów wymiaru sprawiedliwości, albowiem nie sposób pominąć naczelnych zasad, w tym prawa do sprawiedliwego i rzetelnego procesu jak również zasady bezstronnego orzekania.

Analogicznie jak w przypadku organów ściągania, w przypadku pracy wymiaru sprawiedliwości również wyodrębnić można pewien katalog spraw powtarzalnych, o niskim stopniu skomplikowania i zaawansowania, które de facto i tak rozstrzygane są według dokładnie takiego samego modelu orzekania[369]. Idąc zatem śladem rozwiązań przyjętych przez Estonię, zaproponować można wdrożenie systemu umożliwiającego automatyczne orzekanie w sprawach o niskiej społecznej szkodliwości czynów, przy wartości przedmiotu sporu nieprzekraczającej kwoty 5.000 zł, czyli spraw dotyczących najmniej poważnych sporów sądowych, o ile dopuszczalna jest taka kategoryzacja. U nadbałtyckiego sąsiada wprowadzono rozwiązanie nazywane botem-arbitrem, również e-sędzią, który ma bezpośrednio na celu automatyzację procedur sądowych, a ściślej mówiąc użycie SI w systemie wymiaru

[367] K. Rutkowski, *Predictive justice – sprawiedliwość algorytmów* [w:] D. Dajnowicz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E.W. Pływaczewski.(red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku*, 2022, s. 846 i nast.
[368] M. Dymitruk, *Prawo sztucznej inteligencji*, red. Świerczyński M, CH Beck, 2020 s. 275 i nast.
[369] Szerzej: É. Buat-Ménard, „*Predictive" justice: Requirements, risks, and expectations – the experience in France*, „Les Cahiers de la Justice" 2019/2

sprawiedliwości. System estoński bezpośrednio dotyczy spraw, w których wartość przedmiotu sporu nie przekracza 7.000 euro, zaś samo oprogramowanie zostało opracowane przez Ott Velsberga[370]. Model taki bezpośrednio opierałby się na analizie i wymianie danych oraz dokumentów, a maszyna w oparciu o pozyskane dane i uczenie maszynowe wydaje orzeczenie, które poddawane byłoby wstępnej analizie przy wykorzystaniu czynnika ludzkiego, to jest przez sędziego. Dopatrując się pozytywnych aspektów w przyjęciu podobnego modelu orzekania, wskazać bezpośrednio należy na usunięcie zaległości w wokandach sędziów, możliwość skupienia większej uwagi na sprawach skomplikowanych i możliwie głębokiej ich analizie, przy jednoczesnym zminimalizowaniu czasu poświęconego na sprawy o podstawowym stopniu skomplikowania, a także przyspieszenie orzekania w tego typu sprawach, odciążenie sędziów i pracowników sądów w obowiązkach, co przy aktualnej ilości spraw jawi się jako bardzo atrakcyjne[371]. Niemniej jednak wprowadzenie do pracy sędziów systemów pośrednio niezależnych od działania człowieka w sferze, w której poczucie sprawiedliwości i bezstronności są maksymalnie pożądane, budzi wątpliwości z perspektywy zasady skutecznej ochrony sądowej, a także dla niezawisłości sędziowskiej oraz podstawowych zasad procesu, o których wyżej wspomniano[372].

W celu zobrazowania potęgi sztucznej inteligencji, a w zasadzie jej skuteczności, przytoczyć należy wyniki eksperymentu przeprowadzonego pod koniec 2017 roku, zainicjowanego przez studentów Uniwersytetu w Cambridge w Wielkiej Brytanii. W jego przebiegu porównano zdolności prawników oraz sztucznej inteligencji, zaś zadaniem była ocena 750 sporów prawnych związanych z dochodzeniem należności finansowych oraz prawem ubezpieczeń, pod kątem przewidzenia, które z pozwów zostaną oddalone, a które zasługują na uwzględnienie. Wyniki przeprowadzonego w ten sposób eksperymentu, nie pozostawiły wątpliwości co do potęgi i predyspozycji „algorytmicznych prawników", albowiem prawnicy prawidłowo przesądzili 66,3% rozpatrywanych spraw, zaś oprogramowanie osiągnęło skuteczność na poziomie 86,6%[373]. Zasygnalizować jedynie należy, niż wyniki mogłyby diametralnie różnić się w przypadku podjęcia próby oceny spraw bardziej

[370] https://dane.gov.pl/pl/promotion/ott-velsberg?lang=en (dostęp: 02.06.2023 r.)
[371] Szerzej: K. Rutkowski, Predictive justice – sprawiedliwość algorytmów [w:] D. Dajnowicz-Piesiecka (red.), E. Jurgielewicz-Delegacz (red.), E.W. Pływaczewski (red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku,* 2022, s. 846 i nast.
[372] M. Bartoszek, Zastosowanie sztucznej inteligencji w sądownictwie w świetle zasady skutecznej ochrony sądowej, Folia Iuridica Univeristatis Wratislavieninsis
[373] https://legaltechnology.com/2017/10/30/machine-beats-man-in-casecrunch-lawyer-challenge/ (dostęp: 15.06.2023 r.)

skomplikowanych albo po prostu o innym przedmiocie, nie można bowiem zapomnieć, iż zapewne aplikacja została przygotowana pod kątem konkretnej kategorii spraw.

6. Ocena ryzyka zastąpienia zawodów prawniczych przez sztuczną inteligencję

Nie pozostawia wątpliwości prawdziwość stwierdzenia, że rozwój technologiczny wywiera bezpośredni wpływ na funkcjonowanie wszystkich zawodów prawniczych, odnosząc nie tylko pozytywne skutki w sferze zadań tej profesji, ale również pośrednio skutki o charakterze negatywnym. Podsumowanie wyżej poczynionych rozważań oraz podjętych badań w tym zakresie wymaga jednakże podjęcia próby oceny z perspektywy sztucznej inteligencji.

Historia bezpośrednio wskazuje, iż na przestrzeni lat dostrzegalne są mniejsze i większe przeobrażenia, zwłaszcza w sektorze szeroko rozumianych usług. Rewolucja przemysłowa wprost dowodzi, iż praca człowieka w rozumieniu fizycznych działań, co najmniej części może być zastąpiona przez pracę maszyn. To, co jeszcze pół wieku temu było w zasadzie niewyobrażalne w tym zakresie, aktualnie stało się rzeczywistością. Na skutek skonstruowania zaawansowanych urządzeń i maszyn wprowadzono do wielu sektorów innowacyjne rozwiązania umożliwiające zminimalizowanie lub całkowite odejście od pracy człowieka, który niejako został zastąpiony przez urządzenie. Niemniej jednak podkreślenia wymaga fakt, iż każdy z takich przypadków stricte dotyczy pracy fizycznej, o charakterze możliwym do otworzenia przez odpowiednio zaprogramowaną maszynę, w związku z czym zadanie urządzenia jest ułatwione. Pytanie zatem, czy inteligencja, która z natury stanowi atrybut człowieka możliwa jest do zastąpienia? A jeśli tak, to czy sztuczna inteligencja może stanowić zagrożenie dla bytu zawodów prawniczych?

Analiza rynku prawniczego nie pozwala na udzielenie jednoznacznej odpowiedzi na postawione w ten sposób pytania. Zdaje się, iż wykorzystanie uczenia maszynowego w Polsce, zwłaszcza w branży prawniczej aktualnie występuje na nisko zaawansowanym poziomie, co pośrednio uniemożliwia dokonanie precyzyjnej oceny. Potencjał wykorzystania sztucznej inteligencji, zwłaszcza u państw zagranicznych w zasadzie jednoznacznie dowodzi, iż generalnie istnieje możliwość zastąpienia – w skrócie ujmując – ludzkiego umysłu. Innowacyjne rozwiązania zdają się nieustannie zaskakiwać, a sposób wykorzystania algorytmów sztucznej inteligencji bywa nieprawdopodobny, na co wskazują przytoczone w ramach tego rozdziału okoliczności. Aby móc ferować wyroki w zakresie zagrożenia dla bytu zawodów prawniczych w związku z rozwojem sztucznej inteligencji dogłębnej analizie należy

poddać aspekty wspierające stanowisko niezastąpionego charakteru tej grupy zawodowej, a także fakty mogące wskazywać na realne jej zagrożenie. W pierwszej kolejności kategorycznie podkreślić należy, iż nauki prawne zakwalifikowane są do dyscypliny nauk społecznych, co z kolei bezpośrednio wskazuje na udział czynnika ludzkiego w celu realizacji zadań przypisach wprost do tej grupy zawodowej. Nie ma wątpliwości co do tego, iż skuteczne podejmowanie działań adwokata lub radcy prawnego w ramach zlecenia otrzymanego od klienta determinowana jest potrzebą zbudowania zaufania między klientem a prawnikiem, co z kolei jest niemalże niemożliwe do osiągnięcia w odniesieniu do potencjalnych maszyn. Oczywiste jest to, iż zdecydowanie wyższy poziom zaufania przejawiany jest względem człowieka, tym bardziej profesjonalisty, aniżeli względem urządzenia, którego skuteczność w zasadzie nie została stuprocentowo zweryfikowana, natomiast ogólnie przyjęte zaufanie do prawników – jak najbardziej tak. Co więcej, podkreślenia wymaga fakt, iż środowisko prawnicze ulega nieustannym przeobrażeniom i rozwojowi, pojawiają się coraz to nowsze dziedziny prawa, a w konsekwencji specjaliści w tym zakresie. Analogicznie kwestia ta wygląda w zakresie nowelizacji przepisów prawnych oraz wprowadzenia nowych regulacji. Wykładnia przepisów prawnych nie zawsze jest jednolita i oczywista, w doktrynie i orzecznictwie często pojawiają się spory i rozbieżności w tym zakresie, niekiedy trwające nawet latami, zatem ciężko wyobrazić sobie sytuację, w której takie problemy i dylematy mogłyby być rozstrzygane na poziomie maszyn wyposażonych w sztuczną inteligencję, która nawet przy zaawansowanym jej wykorzystaniu, nadal funkcjonuje w jej wąskim rozumieniu. Fakt pojawienia się pandemii w sposób znaczny przyspieszył wprowadzenie naprawdę zaawansowanych rozwiązań technologicznych wśród zawodów prawniczych, powodując, że model udzielania porad prawnych przybrał inny, bardziej zaawansowany wymiar. Sytuacja na rynku, w tym postęp technologiczny niejako wymusza na prawnikach większą produktywność i wydajność, przy jednoczesnym dostarczaniu większych świadomości. Świadomość zagrożenia również nie pozostaje bez znaczenia w tym zakresie.

Niewątpliwie wyżej przytoczone możliwości potencjalnego wykorzystania sztucznej inteligencji wśród wszystkich profesji z zakresu branży prawniczej, a także przywołane wyżej przykłady faktycznego wykorzystania takich urządzeń, nie tylko w państwach wysokorozwiniętych, ale również w państwach sąsiedzkich, wprost determinują konieczność stwierdzenia, iż istnieje ryzyko znacznego wpływu tego innowacyjnego rozwiązania na byt zawodów prawniczych, niemniej jednak nie sposób uznać, iż zagrożenie to ma charakter realny, a wyłącznie potencjalny. Ocena ta może w przyszłości z pewnością ulec modyfikacji na skutek

wprowadzenia coraz to bardziej zaawansowanych rozwiązań, być może również wprowadzenia szerokiej (silnej) sztucznej inteligencji, aczkolwiek poczynione ustalenia dotyczą aktualnej sytuacji rynkowej.

Niezależnie od powyższego, pomimo przytoczenia licznych okoliczności przemawiających za teoretycznym brakiem możliwości zastąpienia prawników przez model uczenia maszynowego, sztucznej inteligencji nie można absolutnie lekceważyć. Bez wątpliwości najbardziej zagrożoną grupą zawodową są adwokaci i radcowie prawni, co wynika wprost z potencjału wynikającego z chatboxów oraz algorytmicznych prawników i udzielania porad prawnych w takim właśnie modelu[374]. Nie można jednak pominąć istotnej funkcji realizowanej przez tą grupę zawodową, a polegającą na reprezentowaniu jednostki przed sądami lub innymi instytucjami, co z kolei jest niemalże niemożliwe do otworzenia według stanu aktualnej wiedzy przez sztuczną inteligencję, podobnie jak spełniana przez prawników rola negocjatora i arbitra. Zatem o ile udzielanie porad prawnych w nieskomplikowanych sprawach, o podstawowym stopniu skomplikowania, niewymagającymi złożonej wykładni przepisów prawnych oraz analizy obszernego orzecznictwa, zdaje się być możliwe do zastąpienia przez uczenie maszynowe, o tyle wszelkie inne sfery działania, o których wspomniano wyżej, w tym również prowadzenie spraw skomplikowanych i wymagających, nie są zagrożone przez świat sztucznej inteligencji.

Nie sposób natomiast sobie wyobrazić zagrożenia dla bytu organów ścigania i wymiaru sprawiedliwości, zatem nawet najbardziej zaawansowane i innowacyjne narzędzia opracowane w dalekiej przyszłości, nie są w stanie w aktualnie panującym porządku prawnym zastąpić pracy sędziego i prokuratora[375]. Ewentualne urządzenia oparte o działanie nowych technologii mogą jedynie wspomóc pracę tej grupy zawodowej oraz ułatwić i jednocześnie udoskonalić realizację przypisanych im zadań. Przytoczone wyżej przykłady możliwości zastosowania sztucznej inteligencji wśród organów ścigania oraz wymiaru sprawiedliwości wprost potwierdzają tę tezę. Przy okazji futurologicznego rozstrzygania kwestii umożliwiających wprowadzenie sztucznej inteligencji, wyraźnie zaznaczyć należy, iż odbywa się to wyłącznie w kategorii hipotetyzowania, albowiem przyjęcie uczenia maszynowego wśród pracy organów ścigania i wymiaru sprawiedliwości nie jest zasadniczo prostym zabiegiem. Nie ma

[374] Szerzej: R. Koch, *Legal Tech i nowoczesne technologie w pracy prawników wewnętrznych* [w:] K. Dzioba. (red.), R. Rybicki (red.), *Metodyka pracy prawnika in-house*, 2021

[375] J. Morison, A. Harkens, *Re-engineerig justice? Robot judges, computerised courts and (semi) automated legal decision-making*, Queen's University Belfast, "Legal Studies" 2019, t. 39, nr 4, s. 618-635

wątpliwości co do tego, iż jest to bardzo złożony proces, o niebywale długotrwałym przebiegu, a jednym z jego elementów jest wprowadzenie specjalnych uregulowań prawnych, zwłaszcza w zakresie ochrony danych osobowych. Wyłącznie stworzenie warunków prawnych w postaci odpowiednio opracowanych regulacji prawnych w postaci konkretnych i jasnych przepisów, pozwoli na zapewnienie bezpieczeństwa rzeczonych rozwiązań, a w konsekwencji poczucia bezpieczeństwa i sprawiedliwości prawnej wśród społeczeństwa.

Mając zatem na względzie powyższe, należy ostudzić emocje serwowane zwłaszcza przez media. Pomimo rewolucji technologicznej, zwanej także czwartą rewolucją przesyłową stosowanie autonomicznych systemów opartych o działanie sztucznej inteligencji nie przyjdzie tak prędko, o ile nadejdzie w ogóle, w odniesieniu do branży prawniczej. Ponownie podkreślić należy, iż podejmowane w ramach czynności zawodowych zadania przez prawników oparte są na stosunku zaufania[376], zaś prawnicy są profesjonalistami kontrolującymi rynek, świadczącymi usługi na profesjonalnym poziomie, zapewniając w ten sposób zbiorowe potrzeby społeczeństwa oraz poczucie sprawiedliwości, które w konkretnych stanach faktycznych może być zagrożone.

[376] S. Thiebes, S. Lins, A. Sunyaev, *Trustworthy artificial intelligence,* "Electronic Markets" 2021, t. 31, nr 2, s. 455

Rozdział VI

Postulaty w zakresie wpływu nowych technologii na zawody prawnicze

Całokształt wyżej przytoczonych faktów i okoliczności w sposób ewidentny potwierdza postawioną na wstępie tezę, zgodnie z treścią której nowe technologie i ich rozwój w sposób bezpośredni i znaczący wpływają na działanie wszystkich zawodów prawniczych. Na kanwie przedmiotowych rozważań, analiza ta przeprowadzona została w zdecydowanej większości na podstawie badań dotyczących działalności szeroko rozumianych organów ścigania. Na przestrzeni ostatnich dziesięcioleci praca zawodów prawniczych uległa znacznej zmianie, w tym modernizacji i informatyzacji. Skrajnym przykładem zdaje się być chociażby fakt, iż niezwykle rzadko, a można byłoby nawet stwierdzić, iż niemożliwe jest spotkanie prawnika, który biegle nie korzystałby z urządzeń elektronicznych, w tym komputerów. To, co jeszcze 3 dekady temu było wybitną rzadkością i spektakularnie nowoczesnym rozwiązaniem – dziś jest normalnością i podstawą. Większość pism procesowych tworzonych i redagowanych jest za pomocą komputera, większość dokumentów ma charakter pisma maszynowego, natomiast komunikacja z klientami również nierzadko odbywa się za pomocą komunikacji na odległość.

Przedstawienie argumentów pozwalających na wyodrębnienie zarówno pozytywnych i negatywnych konsekwencji wpływu postępu technologicznego w odniesieniu do konkretnych zawodów prawniczych może jednak okazać się niezwykle trudne, albowiem z punktu widzenia danej profesji, określony czynnik może być odbierany zupełnie inaczej. Niemniej jednak po przeprowadzeniu analizy w tym zakresie, w pełni celowe jest podjęcie próby dokonania oceny zmian w funkcjonowaniu zawodów prawniczych podyktowanych postępem technologicznym, jak również podjęcie próby zbadania jak kwestia ta może wyglądać w przyszłości. Na tej podstawie z kolei możliwe będzie wyciągnięcie wniosków, a być może sformułowanie także postulatów, które umożliwiłyby w większym stopniu wykorzystanie potencjału nowych technologii oraz dokonanie oceny dotychczas przyjętych rozwiązań udostępnionych przez prawodawcę.

1. Ocena wpływu nowych technologii na organy ścigania

W gruncie rzeczy, na przestrzeni przedmiotowej pracy, wpływ nowych technologii na działalność organów ścigania analizowany i badany był z punktu widzenia cyberbezpieczeństwa i przez ten pryzmat konsekwencje związane z postępem technologicznym zostały ocenione negatywnie.

Nie ma wątpliwości co do tego, iż nowe technologie bezpośrednio wpływają na liczbę cyberprzestępstw popełnianych na terenie kraju, bezpośrednio dyktując sprawcom takich czynów zabronionych nowe metody ich popełnienia, udostępniając coraz to bardziej innowacyjne narzędzia i techniki sprawcze, a tym samym w sposób zdecydowany utrudniając organom ścigania proces wykrywczy takich sprawców i zapewnienie ogólnego cyberbezpieczeństwa. W dużym uproszczeniu zatem, brak postępu technologicznego w zakresie komunikacji elektronicznej i w zakresie sukcesywnego pojawiania nowych środków umożliwiających coraz łatwiejsze popełnienie przestępstw przy wykorzystaniu sieci teleinformatycznej, powodowałby z pewnością nie tylko zahamowanie wzrostu liczby cyberprzestępstw popełnianych na terenie kraju, ale również okoliczność ta odniosłaby bezpośredni wpływ na statystykę w zakresie wykrywalności przestępstw tego rodzaju. Niestety tak pozytywna prognoza przyszłości jest niemożliwa, albowiem niejako zahamowanie rozwoju technologicznego w zakresie wyłącznie cyberbezpieczeństwa jest jedynie abstrakcją, a w ogólnym rozrachunku nie ma wątpliwości co do tego, iż postęp technologiczny jest bardzo potrzebny i pożądany.

Niezależnie od powyższego, nowe technologie oraz komunikacja elektroniczna w sposób zarówno pośredni jak i bezpośredni wpływa na funkcjonowanie szeroko rozumianych organów ścigania. W zdecydowanej większości zmiany w tym zakresie, abstrahując od kwestii cyberprzestępczości, należy ocenić pozytywnie, albowiem wpływają one na znaczne przyspieszenie, usprawnienie i ułatwienie pracy tej profesji. Wśród czynników, które zasługują na pozytywną ocenę bez wątpienia wskazać należy wszelkie bazy danych działające w oparciu o sieć teleinformatyczną, które gromadzą szeroki katalog danych dotyczących m.in. przestępstw i przestępców, które w sposób niewyobrażalny wpływają na pracę organów ścigania. Dzięki nowym technologiom współpraca i komunikacja między organami ścigania przybrała zupełnie inną formę aniżeli w przeszłości. W tym zakresie na zdecydowaną aprobatę zasługuje udostępnienie dla organów ściągania systemu ProkSys, który przybrał jednolitą formę dla wszystkich jednostek prokuratury na terenie kraju, niezależnie od ich szczebla. Program ten, wykorzystujący działanie sieci teleinformatycznej, usprawnia funkcjonowanie organów ścigania nie tylko z punktu widzenia komunikacji z innymi jednostkami, ale również z perspektywy kwestii organizacyjnych, administracyjnych i procesu ścigania sprawców przestępstw.

Sukcesywne doskonalenie możliwości i narzędzi udostępnianych w ramach tego systemu, zdaje się być nieprawdopodobną szansą dla maksymalnego przyspieszenia

i usprawnienia postępowania przygotowawczego, ale również dla ułatwienia pracy organów ścigania. Przykładem, który w sposób doskonały obrazuje pozytywne zmiany w tym zakresie zdaje się być dostęp do Krajowego Rejestru Karnego, który jest nieodłącznym elementem w pracy szeroko rozumianych organów ścigania. Zasygnalizować jedynie należy, iż dostęp do tego narzędzia jest konsekwencją udostępnienia wyżej wspomnianego systemu ProkSys. Pozyskanie kompletnych danych z tego rejestru, prowadzonego również przy wykorzystaniu sieci teleinformatycznej, pozwala na ustalenie wielu okoliczności faktycznych popełnionego czynu zabronionego i jest niezbędne w przypadku kierowania aktu oskarżenia do sądu, który musi posiadać wiedzę na temat uprzedniej karalności oskarżonego, co na etapie postępowania sądowego może mieć wpływ na wymiar kary zgodnie z przyjętymi dyrektywami w tym zakresie, natomiast na etapie postępowania przygotowawczego może determinować uwzględnienie w kwalifikacji prawnej recydywy lub też recydywy wielokrotnej. Dotychczas najszybszą metodą pozyskania danych z rejestru było dokonanie tej czynności przy pomocy Policji, która w ciągu kilku dni miała możliwość poczynienia ustaleń w tym zakresie. Zaskakującym zdaje się być fakt, iż dotychczas prokuratorzy nie mieli bezpośredniego dostępu do rzeczonej bazy danych, której zasoby w rzeczywistości w pierwszej kolejności powinny zostać udostępnione dla tej grupy zawodowej, zwłaszcza, że z punktu widzenia rozwiązań technologicznych nie było w tym zakresie w zasadzie żadnych przeszkód. W związku z udostępnieniem systemu ProkSys, kwestia ta uległa całkowitej zmianie, albowiem aktualnie pracownicy wszystkich jednostek prokuratur posiadający dostęp do przywołanego do systemu mają możliwość pozyskania danych o karalności w ciągu kilku sekund. Oczywiście, w celu zapewnienia maksymalnego bezpieczeństwa udostępnianych danych oraz zapobiegnięciu pozyskania informacji nieprzeznaczonych, dla skutecznego uzyskania informacji z Krajowego Rejestru Karnego niezbędne jest wskazanie sygnatury postępowania przygotowawczego, dla potrzeb którego organ potrzebuje tych informacji, jak również wskazanie danych identyfikujących osobę, co do której kierujemy wniosek o udostępnienie danych. Po prawidłowym wypełnieniu formularza w wersji elektronicznej, po zaledwie kilku sekundach, generowana jest przez system odpowiedź zawierająca bardzo szczegółowe dane dotyczące karalności konkretnej osoby, w tym dokładne wskazanie prawomocnych orzeczeń sądu, którymi dana osoba została skazana, na jaką karę, czy kara została wykonana w całości, czy też jest w trakcie wykonania, a także informacje w zakresie ewentualnego zarządzenia wykonania kary zawieszonej, czy też zamiany kary ograniczenia wolności na karę pozbawienia wolności. Poza wskazanymi informacjami, organy ścigania uzyskują także informację na temat listów gończych, a także zastosowanych izolacyjnych środków zapobiegawczych w postaci

tymczasowego aresztowania ze wskazaniem jednostki, do dyspozycji której konkretna osoba pozostaje.

Wyżej przytoczony przykład w sposób bezpośredni wskazuje na zdecydowanie pozytywną zmianę, która pośrednio podyktowana jest rozwojem nowych technologii i bez istnienia środków komunikacji elektronicznej byłaby niemożliwa lub znacznie utrudniona. Udostępnienie tak podstawowego narzędzia w sposób nieprawdopodobny wpłynęło na komfort pracy tej grupy zawodowej, usprawniając również postępowanie przygotowawcze i wpływając na jego czas trwania. Niemniej jednak dostęp do omawianego rejestru nie jest oczywiście jedyną zaletą postępu technologicznego w odniesieniu do działalności organów ścigania, aczkolwiek z tego, konkretnego punktu widzenia – najbardziej zauważalną i wymagającą zasygnalizowania. Nadmienić nadto należy, iż przywołany system, oprócz powyższego, zapewnia szereg innych możliwości i narzędzi usprawniających działalność organów ścigania i wykorzystujących w swoim funkcjonowaniu nowe technologie, niemniej jednak z punktu widzenia przedmiotowych rozważań, dogłębna ich analiza wymaga odrębnej analizy.

Oprócz wyżej wymienionej nieprawdopodobnej korzyści wynikającej z sukcesywnej informatyzacji działalności szeroko rozumianych organów ścigania, wskazać również można na kolejną zaletę dostarczaną za pomocą wyżej opisanego systemu udostępnionego do pracy prokuratorów i innych pracowników prokuratury. Szczegółowa analiza najbardziej popularnych rodzajów cyberprzestępstw, a w zasadzie analiza algorytmu działania organów ścigania w sposób ewidentny wskazuje na niezwykle istotną rolę instrumentu w postaci postanowienia o żądaniu wydania rzeczy w procesie wykrywczym cybersprawców. Status prawny jak również treść takiego postanowienia została omówiona wyczerpująco w poprzednich rozdziałach. W tym miejscu wskazać jednak należy istotną modernizację wprowadzoną skutecznie na przełomie 2021/2022 r. w ramach wspomnianego systemu ProkSys. Dotychczas w przypadku konieczności procesowego zabezpieczenia i pozyskania wszelkich danych telekomunikacyjnych, po ustaleniu operatora sieci komórkowej, prokurator sporządzał postanowienie o żądaniu wydania rzeczy, które na skutek jego zarządzenia ekspedycyjnego doręczane było właściwemu operatorowi, który po rozpoznaniu postanowienia o żądaniu wydania rzeczy, udostępniał dane telekomunikacyjne, przesyłając je za pomocą operatora pocztowego. Sposób przesyłania, jak również otrzymywania tych danych bezpośrednio wpływał na długi czas oczekiwania, co w konsekwencji przekładało się na długotrwałość postępowań przygotowawczych, w których niezbędne było otrzymanie, a następnie przeanalizowanie ww. danych. Wyjątkiem od rzeczonej zasady, była komunikacja

z operatorem sieci komórkowej P4 Sp. z o.o. (Play), który udostępnił specjalny generator postanowień o żądaniu wydania rzeczy i umożliwiał ich przesyłanie w drodze elektronicznej, co bez wątpliwości wpływało na czas oczekiwania na dane retencyjne od tego konkretnego operatora. Aktualnie jednak sytuacja ta uległa nieprawdopodobnie pozytywnej przemianie, albowiem dla pracy prokuratorów udostępniono obecnie możliwość pozyskania danych retencyjnych w drodze elektronicznej od większości operatorów funkcjonujących na polskim rynku. Obecnie system bazujący na działaniu sieci teleinformatycznej umożliwia nie tylko wysyłanie sporządzonych postanowień o żądaniu wydania rzeczy za pomocą komunikacji elektronicznej, ale również ich wygenerowanie. System umożliwia sporządzenie postanowienia według określonego formularza, gdzie część wypełniana jest automatycznie za pomocą odczytywania danych z systemu bazy danych dotyczących danego postępowania (tj. formy postępowania przygotowawczego, opisu jego przedmiotu, przyjętej kwalifikacji prawnej), następnie prokurator uzupełnia informację dotyczące żądanych danych – konkretnego numeru abonenta, adresu IP wraz z podaniem numeru portu źródłowego, czasu działania w sieci oraz wskazania w jakim zakresie operator ma udostępnić żądane dane. Na tej podstawie system generuje postanowienie o żądaniu wydania rzeczy, którego najistotniejszym elementem jest kod QR będący w następstwie podstawą uzyskania danych retencyjnych. Po patrzeniu postanowienia własnoręcznym podpisem, jest ono skanowane i przesyłane do właściwego operatora sieci komórkowej (również za pośrednictwem systemu ProkSys), który udziela odpowiedzi w ciągu maksymalnie kilku dni, często w ciągu kilku godzin, a nie jak dotychczas – kilku tygodni, a nawet miesięcy. Uzyskane dane otrzymywane są w wersji elektronicznej, w tym m.in. w formie formularza excel, co z kolei w sposób zdecydowany ułatwia przeprowadzenie ich analizy, w tym analiz porównawczych z dotychczas pozyskanymi danymi telekomunikacyjnymi, zestawień oraz powiązań między konkretnymi użytkownikami ustalonych numerów telefonów. Zarówno sposób sporządzenia postanowienia o żądaniu wydania rzeczy, jak również czas oczekiwania na dane telekomunikacyjne oraz sposób ich otrzymania w bezpośredni sposób wpływają na realizację naczelnej zasady procesu karnego, tj. zasadę szybkości postępowania, przyczyniając się do jej realizacji w maksymalnie możliwym stopniu.

Wskazane powyżej przykłady w sposób bezpośredni obrazują jak znaczący wpływ wywiera postęp technologiczny na działalność organów ścigania, pokazując, iż dostarcza on nie tylko wielu zagrożeń zwłaszcza w zakresie cyberbezpieczeństwa, ale również determinując sposób pracy organów ścigania. Przykłady te, oczywiście jako jedne z wielu, pozwalają na

sformułowanie stwierdzenia, iż w związku z nieustannym postępem technologicznym, mamy do czynienia z również regularnie postępującą informatyzacją działalności tej grupy zawodowej. Skoro zatem proces wykrywczy jest jednym z głównych zadań organów ścigania, a jego przebieg uwarunkowany jest dostępem do narzędzi, które dla swojego bytu wymagają szeroko rozumianej komunikacji elektronicznej przyjąć należy, iż nowe technologie są nieodzownym elementem działalności organów ścigania, potrzebnym do możliwie maksymalnego usprawnienia i przyspieszenia przebiegu postępowania przygotowawczego, a w konsekwencji do osiągnięcia jego celów, tj. wykrycia sprawcy przestępstwa oraz zapobiegnięcia ponownemu jego popełnieniu.

Wyraźnie zaznaczyć należy, iż zarówno rodzaj jak i sposób wykorzystania narzędzi pojawiających się w związku z sukcesywnym rozwojem technologicznym, podyktowany jest działaniem prawodawcy i odpowiednich zespołów. Sposób reagowania właściwych organów, zarówno na szczeblu krajowym jak i europejskim, na postęp technologiczny jest jednym z najważniejszych elementów w procesie modernizacji nie tylko działalności zawodów prawniczych, ale całej gospodarki. Uwzględnienie przez prawodawcę w regulacjach prawnych nowoczesnych rozwiązań pozwoli na ich skuteczne i zgodne z prawem wykorzystywanie. Zainicjowanie powstania nowych systemów, narzędzi i elementów bezapelacyjnie w pierwszej kolejności wymaga uregulowania ich prawnego statusu, a następnie możliwie precyzyjnego opracowania schematu ich działania przez odpowiednio przygotowane zespoły specjalistów, a dopiero wówczas ich testowanie i następnie udostępnienie dla poszczególnych grup zawodowych. Powyższy mechanizm w sposób ewidentny wskazuje, iż wyłącznie właściwe i odpowiednio sprawne reagowanie na rozwój nowych technologii stwarza idealne warunki dla maksymalnego wykorzystania potencjału nowych technologii wśród zawodów prawniczych.

Analizie poddać należy kwestię odpowiedniego reagowania prawodawcy na postęp technologiczny w zakresie działalności tej grupy zawodowej. Niestety stwierdzić należy, iż nie zawsze prawodawca odpowiednio szybko reaguje na coraz to nowsze i bardziej doskonałe metody działania sprawców cyberprzestępstw, niejako nie nadążając nad wykorzystywanymi narzędziami, a w konsekwencji nie zapewniając organom ścigania dostępu do środków umożliwiających skuteczne przeprowadzenie procesu wykrywczego. Jakkolwiek zastanowić się jednakże należy jaka w rzeczywistości jest realna szansa właściwego reagowania w tym zakresie uwzględniając chociażby moment powzięcia przez organy ściągania wiadomości o sposobie działania sprawcy. Dane te są pozyskiwane przecież już po popełnieniu czynu zabronionego, zatem po powstaniu jakiejkolwiek szkody po stronie pokrzywdzonego, wobec

czego z tej perspektywy – niewiele mogłoby się zmienić. Niemniej jednak, regularnie organizowane są zespoły gromadzące prokuratorów i informatyków, którzy opracowują możliwie dokładne i jednolite algorytmy działania, bazując na najbardziej popularnych modus operandi sprawców, udostępniając w ten sposób organom ścigania schemat skutecznego i ujednoliconego działania podczas procesu wykrywczego. W zakresie udostępniania przez prawodawcę narzędzi umożliwiających swobodną i sprawną analizę, czy też pozyskanie danych, wskazać należy, iż udostępnienie organom ścigania odpowiednich w tej sferze systemów wymaga ogromnego nakładu czasu oraz nakładu finansowego, w tym długoletnich testów, zapewnienia właściwego bezpieczeństwa i ochrony przekazywanych danych, zsynchronizowania baz danych wielu systemów, ulokowania na właściwych serwerach itp. W związku z czym, chociaż być może prawodawca nie do końca odpowiednio reaguje na zmiany w świecie technologicznym i nie udostępnia odpowiednio szybko organom ścigania właściwych narzędzi, to jednak czyni to – realnie rzecz biorąc – w granicach swoich rzeczywistych możliwości, udostępniając jednak niejako w zamian inne instrumenty ułatwiające działalność tej grupy zawodowej.

2. Postulaty dotyczące modernizacji działalności organów ścigania

Na kanwie przedmiotowych rozważań zdaje się bardzo szeroko omówiono już pozytywne jak i negatywne następstwa postępu technologicznego, zwłaszcza z punktu widzenia pracy szeroko rozumianych organów ścigania, a zwłaszcza prokuratorów. Wyczerpująco omówione i przeanalizowane fakty oraz okoliczności nie pozwalają na dokonanie precyzyjnej oceny wpływu nowych technologii na funkcjonowanie tej grupy zawodowej, albowiem pomimo zdecydowanie licznych ujemnych następstw z perspektywy cyberbezpieczeństwa, w sposób ewidentny dostrzegalne są pozytywne przeobrażenia i modernizacje bezpośrednio wpływające zarówno na organizację pracy organów ścigania oraz przebieg – najistotniejszego z tego punktu widzenia – procesu wykrywczego, w tym sposobu prowadzenia postępowania przygotowawczego. Niemniej jednak, pomimo przywołania szeregu przykładów wskazujących na sukcesywne udoskonalanie pracy organów ścigania, co z kolei bezpośrednio podyktowane rozwojem technologicznym, nie sposób uznać, iż sytuacja w tym względzie jest idealna i nie wymaga dalszego rozwoju.

Analiza dotychczas przyjętych rozwiązań oraz doświadczenie i praca w szeregach organów ścigania jak również przeprowadzenie wyczerpujących badań w tym zakresie pozwala na sformułowanie pewnych postulatów, które w sposób zdecydowany wpłynęłyby na szybkość

postępowania karnego, ale również ułatwiły i usprawniły pracę organów ścigania, nie tylko z punktu widzenia procesu wykrywczego, ale również z punktu widzenia organizacji pracy i administrowania jej. Pomimo względnie sprawnego reagowania prawodawcy na zmiany technologiczne (z punktu widzenia procedury karnej), nie ma w zasadzie wątpliwości co do tego, iż wiele z narzędzi dostępnych w krajach sąsiadujących mogłoby funkcjonować również w polskim procesie karnym. Zorganizowanie właściwego dostępu do rzeczonych narzędzi zdecydowanie przyniosłoby więcej korzyści aniżeli problemów organizacyjnych związanych z wprowadzaniem ich do obrotu. Poniżej przedstawione zostaną najistotniejsze postulaty mogące przyczynić się do znacznego, a nawet kilkukrotnego przyspieszenia przebiegu postępowania przygotowawczego, a nadto do zarówno wykrycia sprawców przestępstw i zapobiegania ich ponownemu popełnianiu.

Jako pierwszy postulat, niebywale istotny z punktu widzenia procesu wykrywczego dotyczącego cyberprzestępstw, związany z pozyskiwaniem danych telekomunikacyjnych, który to etap jest kluczowym w przyjętym algorytmie całego procesu, jest sposób ich procesowego zabezpieczenia i uzyskania. Nie ma wątpliwości co do tego, iż niemalże milowym krokiem naprzód jest udostępnienie prokuratorom narzędzi umożliwiających sporządzenie postanowienia o żądaniu wydania rzeczy do operatorów sieci telekomunikacyjnych w drodze elektronicznej oraz przesłanie rzeczonej decyzji w ten sam sposób, niemniej jednak sam przebieg tego procesu wzbudza wiele wątpliwości, kontrowersji i rodzi pytania czy z praktycznego punktu widzenia, faktycznie ułatwiono pracę organów ścigania, a bez wątpienia winna to być naczelna zasada wszelkich wprowadzanych modernizacji. Zdaje się niewielkie modyfikacje sprawiłyby, iż ten sposób pozyskania danych telekomunikacyjnych mógłby zostać określony mianem doskonałego. Niezależnie od powyższego, jednoznacznie podkreślić należy, iż w zasadzie najważniejszym elementem wprowadzonych zmian jest czas oczekiwania na wnioskowane informacje i bez wątpienia kwestia ta zasługuje na pozytywną ocenę, a żadne udoskonalenia nie są potrzebne w tym zakresie. Wątpliwości natomiast budzi sama procedura zwracania się do właściwego operatora o konkretne dane. O ile sam sposób redagowania postanowienia o żądaniu wydania rzeczy jest zdecydowanie łatwiejszy, co spowodowane jest możliwością odczytania danych dotyczących postępowania przygotowawczego z systemu, o tyle niedogodności pojawiają się przy okazji samego przesyłania rzeczonego postanowienia do właściwego operatora, albowiem dla skutecznego pozyskania danych niezbędne jest uprzednie wydrukowanie wskazanej decyzji, opatrzenie jej podpisem, zeskanowanie docelowo do pliku w formie PDF, a dopiero wówczas wgranie pliku do specjalnie przygotowanej sekcji

i wysłanie go. Okoliczność ta w sposób bezpośredni determinuje fakt, iż samo przygotowanie postanowienia o żądaniu wydania rzeczy oraz jego przygotowanie do wysyłki, a następnie wysyłka jest zdecydowanie bardziej długotrwałe aniżeli samo otrzymanie danych telekomunikacyjnych. Konieczność zeskanowania dokumentu obliguje nawiązanie współpracy i zaangażowanie również pracowników sekretariatu, albowiem nie każdy prokurator wyposażony jest w odpowiedni sprzęt umożlwiający wykonanie tej czynności. Fakt ten w praktyce powoduje pojawie się krytycznych głosów postulujących, iż poprzedni system nie nakładał tylu dodatkowych obowiązków.

W związku z licznie pojawiającymi się wątpliwościami, analizie poddać należy sposoby i środki, które ułatwiłyby i ulepszyły dość obiecujący sposób pozyskania i procesowego zabezpieczenia danych telekomunikacyjnych. Przeprowadzone badania wskazują, iż wyłącznie jeden zabieg spowodowałby maksymalizacje w zakresie czasu pozyskania danych telekomunikacyjnych, a wyraźnie podkreślić należy, iż na kanwie przedmiotowych rozważań wielokrotnie sygnalizowano istotność tego czynnika w przypadku procesu wykrywczego przestępstw popełnianych za pośrednictwem sieci teleinformatycznej. Udostępnienie organom ścigania narzędzia umożliwiającego podpisanie dokumentu w postaci postanowienia o żądaniu wydania rzeczy sporządzonego w wersji elektronicznej za pomocą podpisu o takim samym charakterze, tj. podpisu elektronicznego wyeliminowałoby w zasadzie w zupełności wszelkie niedogodności związane ze skanowaniem i podpisywaniem rzeczonego dokumentu przed jego wysyłką. Współcześnie bardzo często w obrocie prawnym dostrzega się dokumenty podpisane wyłącznie za pomocą podpisu elektronicznego, który to zabieg w całości ocenić należy jako bardzo pozytywny. Być może wprowadzenie tej formy podpisu, chociaż dla celu sprawnej wysyłki postanowień o żądaniu wydania rzeczy, pozwoliłoby na pełne osiągnięcie zamierzeń jakie niosło za sobą udostępnienie dla prokuratorów systemu ProkSys, a w konsekwencji sekcji dotyczącej pozyskania danych telekomunikacyjnych w drodze elektronicznej i komunikacji na odległość. W związku z tym, iż czynność procesowa polegająca na uzyskaniu danych telekomunikacyjnych i sporządzaniu postanowień o żądaniu wydania rzeczy została zastrzeżona przez prawodawcę jako wyłączna kompetencja prokuratora, kwestia bezpieczeństwa posłużenia się podpisem elektronicznym nie powinna w zasadzie budzić wątpliwości, za czym przemawia dodatkowo fakt, iż zarówno formularz postanowienia o żądaniu wydania rzeczy oraz sekcja umożliwiająca jego przesłanie dostępna jest wyłącznie dla użytkowników systemu ProkSys posiadających odpowiedni certyfikat, a nadto pozyskanie danych telekomunikacyjnych możliwe jest wyłącznie przez prokuratora, w referacie którego

znajduje się konkretne postępowanie przygotowawcze. Być może, sukcesywne ulepszanie i modernizowanie przyjętych rozwiązań jak również licznie pojawiające się głosy krytyczne, skłonią prawodawcę do udostępnienia przywołanego wyżej instrumentu, albowiem – jak już powyżej wskazano – jeden zabieg sprawiłby, iż wprowadzony model pozyskania danych telekomunikacyjnych stałby się doskonałym – z każdego punktu widzenia, a nie tylko z perspektywy czasu otrzymania odpowiedzi od operatora sieci telekomunikacyjnej. Korzyści jakie niesie za sobą rzeczone rozwiązanie są nieprawdopodobnie pozytywne z praktycznego punktu widzenia w odniesieniu do nakładów, w tym organizacyjnych niezbędnych do jego wprowadzenia.

Możliwość sformułowania postulatów w zakresie wdrożenia w szerszym zakresie nowych technologii do działalności organów ścigania bezpośrednio związana jest z obserwacją i prowadzeniem badań w tej sferze zawodowej. W procesie wykrywczym dotyczącym w zdecydowanej większości przestępstw popełnianych przy wykorzystaniu sieci teleinformatycznej nieodłącznym elementem bardzo często jest konieczność pozyskania danych objętych tajemnicą bankową. Pozyskanie tych informacji jest równie istotne co zabezpieczenie wyżej wspomnianych danych telekomunikacyjnych, albowiem tylko analiza całokształtu materiału dowodowego zgromadzonego w toku postępowania przygotowawczego daje szanse na ustalenie tożsamości sprawcy czynu zabronionego. Niejednokrotnie zdarzają się również sytuacje, iż dopiero po uzyskaniu danych bankowych możliwe jest wytypowanie danych telekomunikacyjnych, które z kolei mogą doprowadzić bezpośrednio do sprawcy cyberprzestępstwa lub chociażby osoby, która pomogła w jego popełnieniu. Całokształt wyżej przytoczonych okoliczności w sposób bezpośredni podkreśla ważność tego rodzaju danych. Na kanwie poprzednich rozdziałów wyczerpująco omówiono zarówno podstawę prawną jak i sposób aktualnych możliwości pozyskania danych objętych tajemnicą bankową. Przypominając, według aktualnie obowiązującej procedury – w dużym skrócie – niezbędne jest sporządzenie wniosku o zwolnienie z tajemnicy bankowej, który kierowany jest do właściwego wydziału karnego właściwego miejscowo Sądu Okręgowego. Czynność ta jest wyłączną kompetencją prokuratora. Na tej podstawie sąd wydaje postanowienie w przedmiocie zwolnienia z tajemnicy bankowej konkretnej instytucji bankowej w zakresie konkretnego numeru rachunku bankowego oraz uprzednio wnioskowanych informacji. Po uzyskaniu rzeczonego postanowienia, prokurator przesyła je do właściwego banku lub instytucji bankowej i dopiero na tej podstawie udostępniane są wnioskowane dane. Cała procedura jest złożona, skomplikowana i co najbardziej istotne – bardzo długotrwała. Praktyka wskazuje, iż czas

oczekiwania na dane objęte tajemnicą bankową, które w większości przypadków zdają się być kluczowe w przypadku cyberprzestępstw, albowiem niejednokrotnie pozwalają na pociągnięcie do odpowiedzialności karnej co najmniej osoby pomagającej w popełnieniu tego rodzaju przestępstwa, licząc od momentu złożenia wniosku do Sądu Okręgowego do czasu faktycznego otrzymania żądanych danych liczony jest w miesiącach i zazwyczaj wynosi około 3 miesięcy. Dla refleksji warto wskazać, iż ustawowy czas trwania dochodzenia, które jest zdecydowanie częściej występującą formą postępowania przygotowawczego, wynosi 2 miesiące. Nie ma co prawda wątpliwości co do tego, iż dane bankowe objęte są nieco „poważniejszą" tajemnicą aniżeli dane telekomunikacyjne, ale ta kategoryzacja w żaden sposób nie jest przeszkodą do wprowadzenia zmian w tym zakresie. Dla ujednolicenia przedstawianych poglądów wskazać należy, iż aktualnie cała procedura pozyskania danych bankowych odbywa się w formie papierowej, z jakimkolwiek pominięciem systemów wykorzystujących sieć teleinformatyczną. Czy wprowadzenie modernizacji tej procedury byłoby bardzo skomplikowane? Jak daleko idące byłyby zmiany podjęte przez prawodawcę? Z praktycznego punktu widzenia, cały proces mógłby zostać opracowany w sposób bardzo zbliżony do pozyskania danych telekomunikacyjnych. Właściwe wydziały sądów okręgowych mogłyby przyjmować wnioski od organów ścigania w drodze elektronicznej i po przeprowadzeniu w tym zakresie posiedzenia, w tej samej formie udostępniać wydane w tym zakresie postanowienia, które z kolei za pomocą wcześniej omawianego systemu ProkSys mogłyby być przesyłane również drogą elektroniczną do właściwych instytucji bankowych. Sam obrót dokumentów w wersji elektronicznej w sposób znaczny przyspieszyłby omawianą procedurę i być może skróciły ją nawet o połowę. Oczywiście wśród praktyków powszechna jest świadomość konieczności oczekiwania na konkretne dane wchodzące w skład materiału dowodowego, niemniej jednak w dobie informatyzacji, skoro jest jakakolwiek możliwość i szansa na usprawnienie tego procesu, dlaczego by takiej szansy po prostu nie wykorzystać. Obieg dokumentów za pośrednictwem operatora pocztowego w wersji tradycyjnej bezpośrednio wpływa na długotrwałość tego procesu, zatem przekazywanie ich za pomocą komunikacji na odległość bez wątpienia skróciłoby ten skomplikowany proces. Być może zbyt daleko idąca wyobraźnia a raczej nierealne marzenie i wizja doskonale zorganizowanego postępowania przygotowawczego, przy maksymalnym wykorzystaniu potencjału nowych technologii prowadzi do ukształtowania pomysłu stworzenia pewnej bazy danych bankowych, silnie zinformatyzowanej, która po odczytaniu treści konkretnego postanowienia sądu okręgowego w przedmiocie zwolnienia z tajemnicy bankowej przesłanego w wersji elektronicznej, generowałaby plik zawierający żądane dane i udostępniała je niemalże automatycznie. Drugi

z przedstawionych poglądów zdaje się być zbyt daleko idącym, niemniej jednak pierwszy postulat z pewnością jest możliwy do osiągnięcia w najbliższym czasie, przy wykorzystaniu dotychczas udostępnionych narzędzi wykorzystujących działanie nowych technologii. Zgodnie z przeprowadzonymi badaniami oraz uzyskanymi wynikami i ich analizą, w toku gromadzenia materiału dowodowego w przypadku cyberprzestępstw najbardziej długotrwałym elementem, bezpośrednio determinującym czas trwania całego postępowania przygotowawczego, jest właśnie pozyskanie danych objętych tajemnicą bankową. Zatem realne skrócenie tego procesu w sposób znaczny wpłynęłoby na realizację postulatu szybkości postępowania karnego pozwalając niejednokrotnie na ukończenie dochodzeń w przewidzianym ustawowo terminie 2 miesięcy, bez konieczności nawet kilkukrotnego jego przedłużania. W zakresie ewentualnych zmian przepisów prawnych regulujących tą dziedzinę, w zupełności wystarczające byłoby bardziej precyzyjne uregulowanie kwestii szeroko rozumianej komunikacji elektronicznej oraz dopuszczenie możliwości komunikowania się w ten sposób również w procesie gromadzenia materiału dowodowego, w tym uzyskania danych objętych tajemnicą bankową.

Kolejnym, równie istotnym postulatem, bezpośrednio związanym z poprzednio omawianymi danymi objętymi tajemnicą bankową, a nieco mniej związanym *stricte* z działalnością nowych technologii, aczkolwiek ściśle związanym z procesem wykrywczym cybersprawców jest sposób pozyskania konkretnych danych bankowych. Jak wyżej wskazano, w celu uzyskania tego rodzaju danych niezbędne jest uzyskanie uprzedniego zwolnienia w tym zakresie z obowiązującej tajemnicy bankowej. Ustawodawca jednak w ustawie Prawo bankowe przewidział wyjątki, które umożliwiają pozyskanie pewnych danych bez posiadania uprzedniego zwolnienia – wymagane jest wyłącznie postanowienie o żądaniu wydania rzeczy. Możliwość taka dopuszczona została m.in. w przypadku, kiedy postępowanie przygotowawcze znajduje się w fazie *in personam*, a dane bankowe bezpośrednio dotyczą podejrzanego w sprawie. W odniesieniu do podmiotów gospodarczych i prowadzonych na ich rzecz rachunków bankowych również nie jest wymagane skierowanie do sądu okręgowego wniosku o zwolnienie z tajemnicy bankowej. Nie ma wątpliwości co do tego, iż w omawianym procesie najdłużej trwającym elementem jest rozpatrywanie wniosku przez sąd okręgowy oraz przekazanie postanowienia do właściwej instytucji bankowej. Poza wyżej szczegółowo omówionym postulatem gwarantującym przyspieszenie postępowania karnego istnieje kolejna możliwość ułatwienia pozyskania tego charakteru danych. Rozszerzenie przez ustawodawcę katalogu sytuacji, w których nie jest wymagane uzyskanie zwolnienia z tajemnicy bankowej z pewnością przyczyniłaby się do realizacji w większym stopniu celów postępowania

przygotowawczego. Sformułowanie przepisów, które umożliwiałyby instytucjom bankowym udostępnienie organom ścigania bez uprzedniego zwolnienia z tajemnicy bankowej wyłącznie podstawowych danych w postaci danych osobowych i teleadresowych dysponenta danego (ustalonego w toku postępowania przygotowawczego) numeru rachunku bankowego w sposób zdecydowany przyspieszyłoby czas trwania tego postępowania. Wielokrotnie w przypadku cyberprzestępstw, po ustaleniu numeru rachunku bankowego, na który wytransferowano środki finansowe z rachunku pokrzywdzonego, czy też rachunku bankowego, który wykorzystano przy zawarciu umowy pożyczkowej podszywając się pod inną osobę, w pełni wystarczające jest ustalenie danych dysponenta bez konieczności posiadania historii transakcji, dokumentów dotyczących otwarcia rachunku, pełnomocnictw czy wykazu logowań do interfejsu bankowości elektronicznej. Dopuszczenie przez ustawodawcę takiej możliwości w zdecydowany sposób ułatwiłoby organom ścigania proces wykrywczy. Po uzyskaniu podstawowych danych, prokurator prowadzący dane postępowanie, na podstawie analizy całokształtu materiału dowodowego w powiązaniu z ustalonymi okolicznościami faktycznymi miałby ewentualną możliwość podjęcia decyzji co do konieczności rozszerzenia już posiadanych danych – już w trybie uprzedniego uzyskania postanowienia w przedmiocie zwolnienia z tajemnicy bankowej.

Całokształt wyników badań przedstawionych w niniejszej pracy, zwłaszcza analiza algorytmu działania organów ścigania w procesie wykrywczym sprawców cyberprzestępstw podkreśla istotne znaczenie szeroko rozumianych danych telekomunikacyjnych w skutecznym realizowaniu celów postępowania przygotowawczego. W tym przypadku przez dane telekomunikacyjne rozumieć należy nie tylko dane retencyjne pozyskane od operatorów sieci komórkowych, tj. dane dotyczące numerów IP oraz numerów abonenckich i powiązanych z nimi informacjami, ale do katalogu tego należy zaliczyć również wszelkie dane pochodne pozyskane m.in. od administratorów domen poczty elektronicznej, od administratorów portali społecznościowych, platform sprzedażowych, komunikatorów społecznościowych itp. Przy omawianiu kwestii postulatów dotyczących możliwie największego wykorzystania nowych technologii analizie poddać należy również kwestię współpracy organów ścigania z rzeczonymi podmiotami. W celu zobrazowania możliwości ulepszenia tej sfery, zasygnalizować jedynie w tym miejscu należy, iż aktualnie procesowe zabezpieczenie tego typu materiału dowodowego zgodnie z obowiązującymi przepisami odbywa się poprzez wydanie postanowienia o żądaniu wydania rzeczy i na tej podstawie administratorzy udostępniają żądane dane. Aktualnie istnieje co prawda możliwość zwrócenia się do niektórych z ww. podmiotów w formie elektronicznej, niemniej jednak nie wpływa to bezpośrednio na faktyczny czas uzyskania tych informacji,

a wyłącznie skraca czas komunikacji. Nadto system dotyczący współpracy elektronicznej w tym zakresie nie jest w żaden sposób ujednolicony, wielokrotnie podjęcie próby nawiązania kontaktu – zwłaszcza z operatorami administrowanymi przed podmioty zagraniczne, tj. Snapchat, Discord, AnyDesk – odbywa się na zasadzie metody prób i błędów, wyrażając przekonanie, iż ustalony adres poczty elektronicznej umożliwi skuteczną komunikację z danym podmiotem. Fakt ten bezpośrednio wpływa na długi czas oczekiwania na żądane dane, a w konsekwencji jest to kolejny z elementów przekładający się na czas trwania postępowania przygotowawczego i jego nieukończenie w ustawowym terminie. Istnieje jednak rozwiązanie, które rozwiązałoby zdecydowaną większość problemów i wątpliwości pojawiających się w praktyce w tym zakresie polegające na ujednoliceniu sposobu współpracy. Doskonałym narzędziem byłoby sporządzenie jednolitego, jasnego i precyzyjnego katalogu adresów umożliwiających kontakt z tymi podmiotami w wersji elektronicznej, co usunęłoby wszelkie wątpliwości przy wyborze metody i rodzaju komunikacji. W związku z tym, iż administratorzy zarówno domen internetowych, portali i komunikatorów społecznościowych oraz platform sprzedażowych przechowują, gromadzą i przetwarzają dane użytkowników w bazach wykorzystujących działanie sieci teleinformatycznej, przesłanie w tej formie postanowienia o żądaniu wydania rzeczy mogłoby niejako zautomatyzować i w istotny sposób zinformatyzować udostępnienie tych danych, co pozwoliłoby na ich uzyskanie w ciągu kilku dni, a nawet kilku godzin, przy przyjęciu, iż odpowiedzi również nadsyłane byłyby w wersji elektronicznej. Z daleko sięgającej wyobraźni uznać należy, iż zupełnie idealnym rozwiązaniem byłoby generowanie postanowień o żądaniu wydania rzeczy w formie elektronicznej na ogólnoprzyjętych formularzach, co z kolei umożliwiałoby kreowanie kodów QR. Otrzymanie decyzji w takiej formie, umożliwiłoby systemom odpowiednio opracowanym przez administratorów wyżej wspomnianych podmiotów w zasadzie automatyczne udostępnienie żądanych danych, nawet w ciągu kilku minut od wysłania postanowienia o żądaniu wydania rzeczy.

Na tle rozprawy, zwłaszcza przy okazji zagadnień teoretycznych wyczerpująco omówiono tematykę baz danych wykorzystujących działanie sieci teleinformatycznej oraz ich znaczenie w procesie wykrywczym. Aktualnie stopień zaawansowania wykorzystania nowych technologii w pracy organów ścigania pozwala na wykorzystanie wspomnianych baz danych w zasadzie na każdym etapie postępowania przygotowawczego – czy to w fazie *in rem* czy też w fazie *in personam.* Przeprowadzone badania oraz kompleksowa analiza sposobu oraz algorytmu prowadzenia postępowań przygotowawczych prowadzonych w sprawach dotyczących szeroko

rozumianych oszustw internetowych w sposób ewidentny wskazują na wykorzystanie rzeczonych zbiorów informacji w celu sprawnego prowadzenia dochodzenia albo śledztwa oraz skutecznego wykrycia sprawcy cyberprzestępstwa. Za pomocą baz danych, które gromadzą, przechowują i przetwarzają konkretne informacje można m.in. ustalić rejestracje procesowe ustalonego numeru telefonu, numeru rachunku bankowego, adresu poczty elektronicznej czy nawet konkretnej platformy internetowej służącej do inwestowania w kryptowaluty czy na giełdzie. Oznacza to, że wprowadzając ustalone w toku postępowania przygotowawczego wyżej wymienione dane do wyszukiwarki konkretnej bazy danych można ustalić czy z wykorzystaniem określonej zmiennej toczy się lub toczyło postępowanie przygotowawcze w innych jednostkach na terenie kraju, czy zostało już zakończone – a jeśli tak to w jaki sposób, jaka jest jednostka właściwa do prowadzenia postępowania oraz sygnatura (zazwyczaj policyjna) danego postępowania. Poczynienie tych ustaleń wielokrotnie okazuje się bardzo przydatne w toku postępowania, co uwarunkowane jest wieloma przyczynami. Po pierwsze, ustalenie rejestracji procesowych danego rachunku bankowego lub numeru telefonu itp. Może dostarczyć prowadzącemu postępowanie informacji czy w rzeczywistości wcześniej był on notowany, a tym samym oznaczać to może, iż był on wykorzystywany dla celów przestępczych. Wówczas w celu pozyskania dodatkowych informacji mogących przyczynić się do wykrycia sprawcy przestępstwa, organy ścigania mają możliwość zwrócenia się do właściwych jednostek policji czy ten prokuratur na terenie kraju w celu uzyskania informacji oraz wiedzy na temat poczynionych ustaleń w zakresie nadzorowanego przez nich postępowania, w toku którego *de facto* wykorzystano np. ten sam numer telefonu.

Zasięgnięcie informacji od innych jednostek może być również przydatne z perspektywy przyspieszenia czasu trwania postępowania, albowiem w przypadku ustalenia rejestracji procesowych rachunku bankowego, od innych jednostek można uzyskać informację na temat jego dysponenta – bez konieczności kierowania do Sądu Okręgowego wniosku w przedmiocie zwolnienia z tajemnicy bankowej. Nadto za pomocą pozyskanych w ten sposób informacji istnieje możliwość ustalenia czy w innych jednostkach jest lub było prowadzone postępowanie zbiorcze, to jest takie postępowanie, które składa się z wielu postępowań przygotowawczych uprzednio prowadzonych przez różne jednostki na terenie całego kraju, które ze względu na tożsame *modus operandi* czy też łączność podmiotową lub przedmiotową zostały połączone do wspólnego prowadzenia mając na względzie m.in. zasadę ekonomiki procesowej. Taka informacja z kolei może pozwolić organom ścigania przekazanie akt głównych danej sprawy do jednostki prokuratury nadzorującej konkretne postępowanie

wykazujące łączność podmiotową lub przedmiotową w celu rozważenia połączenia do wspólnego prowadzenia. Z praktycznego punktu widzenia, analiza wyników przeprowadzonych badań wskazuje, iż prowadzenie postępowania zbiorczego przez jedną jednostkę nadzorującą w większym stopniu pozwala na osiągnięcie celów postępowania przygotowawczego aniżeli odrębne prowadzenie każdego z nich. Przyczynia się to m.in. do zdecydowanie łatwiejszego ustalenie okoliczności faktycznych oraz gromadzenie kompletnego materiału dowodowego w sprawie, co z kolei w sposób bezpośredni wpływa na sposób oraz rezultaty prowadzonego postępowania przygotowawczego.

Całokształt wyżej przytoczonych wyników badań oraz ich analiza w sposób bezpośredni wskazuje na istotny charakter wspomnianych baz danych. Niemniej jednak z faktyczną weryfikacją oraz ustaleniem rejestracji procesowych uprzednio pozyskanych danych w praktyce pojawiają się liczne problemy. W pełni niezrozumiałe jest udostepnienie tego rodzaju systemów wykorzystujących działanie sieci teleinformatycznej w zdecydowanej większości wyłącznie dla funkcjonariuszy policji, nie wyposażając w ten instrument prokuratorów czyli podmiotów *de facto* nadzorujących i wytaczających kierunek działania postępowaniom. Okazuje się zatem, iż prokuratorzy nie mają bezpośrednio możliwości ustalenia rejestracji procesowych rachunków bankowych, numerów telefonów itp., a mogą to wyłącznie uczynić „za pośrednictwem" funkcjonariuszy Policji, zwracając się w wytycznych z poleceniem poczynienia ustaleń w tym zakresie. Nie ma wątpliwości co do tego, iż zabieg ten ewidentnie wpływa na czas trwania postępowania przygotowawczego, natomiast umożliwienie prokuratorom dostępu do baz danych i wyszukiwarek usprawniłoby przebieg całego procesu karnego. Reasumując poczynione rozważania udostępnienie prokuratorom jako podmiotom nadzorującym postępowanie przygotowawcze baz danych umożliwiających za pomocą sieci teleinformatycznej gromadzenie, uzupełnianie materiału dowodowego oraz dokonywanie ustaleń faktycznych jest kolejnym postulatem, który przy wykorzystaniu nowych technologii w sposób zdecydowany poprawiłby jakość pracy organów ścigania. Niemniej jednak udostępnienie po wielu latach do dyspozycji prokuratorów dostępu do baz danych Krajowego Rejestru Karnego daje nadzieje na to, że w przyszłości również na możliwość korzystania pozostałych baz danych.

Przy okazji omawiania postulatów bezpośrednio związanych z nowymi technologiami należy zwrócić uwagę również na narzędzia i metody, które pozwoliłyby na poczucie zdecydowanie większego bezpieczeństwa w sieci a jednocześnie zmniejszyłyby ilość cyberprzestępstw popełnianych na terenie kraju lub co najmniej utrudniły sprawcom tego typu

czynów zabronionych ich skuteczne popełnienie. W związku z omawianiem algorytmu działania organów ścigania w procesie wykrywczym oraz analizy danych, w odniesieniu do których ustawodawca umożliwia ich procesowe zabezpieczenie i uzyskanie, wskazywano na pewne upośledzenie baz danych rejestrujących dane użytkowników MSISDN a w zasadzie przepisów prawnych regulujących tę kwestię. Przypominając, w aktualnie obowiązującym stanie prawnym, co nadal uznawane jest jako nowe, ustawodawca przewidział obowiązek rejestracji kart SIM, co w skrócie oznacza, iż każdy numer telefonu przypisany jest do konkretnej osoby, która rejestrując numer obowiązana jest podać swoje dane osobowe w postaci co najmniej imienia i nazwiska oraz numeru ewidencyjnego PESEL. Bazy danych w tym zakresie przewidują również możliwość gromadzenia informacji dotyczących adresu zamieszkania użytkowników numeru telefonu. Przeprowadzone badania w zakresie narzędzi wykorzystanych przez sprawców w celach przestępczych wskazują, iż pomimo nieustannego rozwoju technologicznego, posługiwanie się połączeniami głosowymi, a w konsekwencji numerami telefonów nadal jest jednym z najbardziej popularnych metod. W związku z tym pozyskanie danych retencyjnych zwłaszcza w odniesieniu do danych osobowych użytkownika numeru telefonu jest podstawowym elementem procesu wykrywczego. Niestety, wyniki badań w tym zakresie nie przedstawiają się obiecująco, albowiem w większości przypadków pozyskanie danych osobowych użytkownika, na którego zarejestrowano numer telefonu jest nieprzydatne z punktu widzenia ustalenia tożsamości sprawcy przestępstwa. Przyczyną tego zjawiska jest przede wszystkim fakt rejestrowania przez sprawców numerów telefonów na przypadkowe osoby, które po uzyskaniu symbolicznej zapłaty, udostępniają swoje dane – niejednokrotnie nie posiadając wiedzy i świadomości na temat faktycznego ich wykorzystania. Problem ten dotyczy zwłaszcza osób bezdomnych, które ze względu na życie w ubóstwie nie podejmują jakiejkolwiek próby zastanowienia się nad celowością i bezpieczeństwem udostępnianych danych. Niezwykle popularnym zjawiskiem jest również rejestrowanie kart SIM na fałszywe dane, podając w rzeczywistości nieprawdziwy lub przypisany do innej osoby numer ewidencyjny PESEL. Powyższe przykłady w sposób bezpośredni prowadzą do wniosku, iż nawet skuteczne uzyskanie danych telekomunikacyjnych od właściwego operatora sieci komórkowej nie daje żadnych gwarancji na ustalenie chociażby ogniwa przestępczego procederu.

Przytoczone wyżej wyniki badań w sposób ewidentny wskazują na nieprawidłowo uregulowane kwestie dotyczące obowiązku rejestrowania numerów telefonów. O ile samo wprowadzenie rzeczonego obowiązku należy ocenić bardzo pozytywnie, o tyle za niezbędne

uznać należy wprowadzenie modyfikacji przepisów prawnych regulujących tą sferę. Dla faktycznego osiągnięcia celu, dla którego *de facto* wprowadzono przedmiotowe regulacje, niezbędne jest zintensyfikowanie weryfikacji przyjmowanych danych w zakresie rejestracji użytkowników. O ile w przypadku podawania fałszywych danych osobowych w postaci numeru ewidencyjnego PESEL sytuacja nie zdaje się być skomplikowana, albowiem wymagane byłoby wyłącznie zastosowanie w systemach baz danych narzędzia umożliwiającego weryfikację spójności numeru PESEL z podanym numerem i nazwiskiem, o tyle w przypadku rejestracji dokonywanych na tzw. „słupów" problem jest nieco bardziej złożony, albowiem w zasadzie podawane dane są przecież prawdziwe. Być może konieczność każdorazowego okazywania dowodu tożsamości oraz skanowania go przez podmioty rejestrujące jak również wyznaczenie do tego celu specjalnych instytucji upoważnionych do weryfikacji, które wyposażone byłyby w instrumenty umożlwiające weryfikację w większym stopniu aniżeli teraz – skutecznie zniechęciłaby sprawców przestępstw do wykorzystywania wyżej opisanych procederów w celu popełnienia czynów zabronionych.

Zmiany przepisów prawnych wymagane są bezapelacyjnie nie tylko w wyżej wyczerpująco omówionej sferze, ale również płaszczyzna dotycząca regulacji prawnych dotyczących danych, które operatorzy sieci komórkowej oraz administratorzy stron internetowych i portali społecznościowych są obowiązani przechowywać. Na tle poprzednich rozdziałów dogłębnej analizie poddano nie tylko sposób pozyskania danych telekomunikacyjnych od wyżej wymienionych podmiotów, ale również przedstawiono katalog danych, co do których istnieje faktyczna możliwość ich procesowego zabezpieczenia. Analiza wyników przeprowadzonych badań jak również poczynione ustalenia na w sposób ewidentny pokazują, iż zakres przechowywanych i przetwarzanych oraz następnie udostępnianych danych jest zdecydowanie zbyt wąski i niewystarczający z punktu widzenia skutecznego wykrycia sprawcy przestępstwa. Największy paradoks polega na tym, iż wskazane podmioty nie mają obowiązku przechowywać danych w postaci numeru portu przy okazji logowania oraz numeru IP (dotyczy to zwłaszcza portali społecznościowych), natomiast dla skutecznego pozyskania pełnych danych dotyczących użytkownika IP operatorzy sieci komórkowych wymagają nie tylko dokładnego czasu działania w sieci z dokładnością do sekundy (gg:mm:ss), ale przede wszystkim numeru portu źródłowego, a niekiedy również numeru portu docelowego. Przykład ten wskazuje na oczywisty brak konsekwencji prawodawcy w tym zakresie lub też brak właściwego nadążania nad postępem technologicznym i zmiennymi niezbędnymi do pozyskania określonych danych. Mając na względzie powyższe, niezbędne jest zatem

ujednolicenie regulacji prawnych dotyczących omawianej sfery i sformułowanie ich w sposób, który w praktyce umożliwi pozyskanie takich danych, które będą danymi istotnymi z procesowego punktu widzenia oraz z punktu widzenia materiału dowodowego i które w konsekwencji mogą przyczynić się do ustalenia tożsamości sprawcy przestępstwa. O ile w pełni należy zgodzić się, iż zakres informacji przechowywanych przez rzeczonych usługodawców jest szeroki, niemniej jednak bez wątpienia nie jest dostosowany do aktualnej sytuacji związanej z postępem technologicznym i wymaga modernizacji w celu zapewnienia maksymalnej ich przydatności w toku postępowania karnego. Przy okazji prezentowania wyników badań w tym zakresie, zasygnalizować jedynie należy, iż w praktyce wśród organów ścigania wskazuje się na wątpliwości dotyczące retencji danych, tj. okresu, przez który usługodawcy obowiązani są przechowywać omawiane dane zwanymi telekomunikacyjnymi. W Polsce prawodawca określił okres retencji na rok. Kontrowersje pojawiają się w odniesieniu do tego czy rzeczony okres jest wystarczająco długi, albowiem wielokrotnie zdarzają się sytuacje, kiedy organy ścigania pozbawione są możliwości pozyskania danych retencyjnych z uwagi na upływ okresu, o którym mowa wyżej. Niejednokrotnie chociażby rachunki bankowe wykorzystywane są dla szeregu przestępstw popełnianych na terenie kraju od zdecydowanie dłuższego okresu niż rok. O ile organy ścigania mają możliwość pozyskania danych bankowych za ten okres, w postaci danych dotyczących dysponenta rachunku bankowego, względnie wykazu transakcji, o tyle udostępnienie przez instytucje bankową adresu IP wykorzystanego podczas utworzenia rachunku bankowego w zasadzie pozbawione jest sensu, albowiem z uwagi na retencje danych operatorzy sieci komórkowej nie udostępnią żądanych danych nawet pomimo sporządzenia postanowienia o żądaniu wydania rzeczy w tym zakresie, dlatego też często odstępuje się od tej czynności procesowej jako pozbawionej znaczenia dla materiału dowodowego. Niemniej jednak, pomimo licznych kontrowersji i wątpliwości w tym zakresie, przychylnie ocenić należy czas retencji danych przewidziany przez ustawodawcę, albowiem z praktycznego punktu widzenia jest on w zupełności wystarczający dla potrzeb postępowania przygotowawczego, a wszelkie niedogodności w tym zakresie mają w zasadzie charakter incydentalny.

Nadmienić nadto należy, iż analiza wyników przeprowadzonych badań wskazuje, że rejestrowanie numerów telefonów na przypadkowe osoby czy też na dane osób w rzeczywistości nieistniejących, ma o wiele dalej sięgające konsekwencje i wywiera niezwykle ujemny wpływ na cyberbezpieczeństwo. Wielokrotnie zdarzają się sytuacje, iż te numery kolejno wykorzystywane są w celu utworzenia rachunków bankowych za pomocą

komunikacji elektronicznej, zawarcia umów pożyczkowych przez Internet itp. Oczywiście nie jest to wówczas jedyny punkt zaczepienia dla organów ścigania, albowiem sprawca pozostawia znacznie więcej śladów w sieci teleinformatycznej, niemniej jednak pozyskanie danych dotyczących numeru telefonu jest zazwyczaj pierwszą wykonywaną czynnością procesową.

Nie bez powodu te kwestie zostały poddane analizie formalnoprawnej jak również praktycznej niemalże na końcu rozważań bezpośrednio odnoszących się do postulatów, które – przy wykorzystaniu nowych technologii – mogłyby przyczynić usprawnienia i przyspieszenia postępowania karnego jak również maksymalizacji skuteczności wykrycia sprawców cyberprzestępstw. O ile w przypadku pozostałych postulatów, ich wprowadzenie nie wymaga spektakularnych zmian systemowych a ich wprowadzenie wydaje się stosunkowo oczywiste w niedalekiej przyszłości, o tyle w przypadku ostatniego z omawianych – zmiany mogą okazać się trudne do wprowadzenia, albowiem niezbędna byłaby zmiana zarówno na płaszczyźnie przepisów prawnych jak również dotychczas funkcjonujących systemów i baz danych gromadzących informację na temat użytkowników numerów MSISDN.

W zakresie większej weryfikacji podawanych przez sprawców danych, która pozwoliłaby na zmniejszenie ilości cyberprzestępstw popełnianych na terenie kraju wymienić należy postulat szerszej weryfikacji prawdziwości ze stanem faktycznym podawanych danych przy okazji zawierania umów pożyczkowych przez Internet. Statystyka wskazuje, iż podszycie się pod inne osoby w takich przypadkach, jest niezwykle popularnym przestępstwem, powodującym duże szkody finansowe po stronie pokrzywdzonego. Oczywiście możliwość błyskawicznego zawarcia umowy pożyczkowej, o ile czyni to faktyczny pożyczkobiorca, należy ocenić pozytywnie, albowiem unika się wszelkiej dokumentacji i obiegu dokumentów, o tyle z punktu widzenia cyberprzestępczości – zdaje się być bardzo niebezpieczne. Posiadanie czyjegoś numeru i serii dokumentu tożsamości oraz numeru PESEL otwiera w zasadzie nieograniczoną możliwość zawarcia na dane określonej osoby zarówno umów pożyczkowych, jak również np. umów o świadczenie usług telekomunikacyjnych. Wprowadzenie dla instytucji bankowych umożliwiających zawarcie umów o pożyczkę przy wykorzystaniu komunikacji na odległość oraz dla operatorów sieci komórkowych narzędzi umożliwiających większą weryfikację klientów z pewnością zmniejszyłaby ilość cyberprzestępstw związanych z tą sferą. Co prawda instytucje bankowe przy okazji zawierania umów pożyczkowych czy też umów o zakupy ratalne przewidują możliwość weryfikacji pożyczkobiorcy polegającą na wykonaniu tzw. przelewu weryfikacyjnego, co ma być potwierdzeniem podanych przez klienta danych i ich spójnością z danymi dotyczącymi rachunku bankowego, z którego takiego przelewu

weryfikacyjnego dokonano. Niemniej jednak kwestia ta okazuje się nie być żadną przeszkodą dla sprawców cyberprzestępstw, albowiem skoro dysponują danymi potencjalnego pokrzywdzonego umożliwiającego im zawarcie umowy pożyczkowej, to również dysponują w zupełności wystarczającymi danymi pozwalającymi na zawarcie umowy o utworzenie rachunku bankowego przez Internet na tego samego pokrzywdzonego. Połączenie tych dwóch faktów daje sprawcom możliwość w zasadzie bezproblemowego pozyskania środków finansowych na szkodę pokrzywdzonego.

Powyżej przytoczono wyłącznie kilka postulatów, które w nieprawdopodobny sposób zmieniłyby szeroko rozumianą pracę organów ścigania. Nie ma absolutnie wątpliwości co do tego, iż pomysłów na udoskonalenie systemu pracy tej grupy zawodowej jest zdecydowanie więcej, albowiem nowe technologie dostarczają szerokiego katalogu możliwości i ich potencjał ocenić należy jako znamienny we wszystkich grupach zawodowych, z pewnością nie tylko szeroko rozumianej działalności prawniczej. Nie da się ukryć, iż zastosowanie i przyjęcie wszystkich z postulowanych narzędzi sprawiłoby, iż czas trwania postępowań przygotowawczych prowadzonych na terenie kraju, zwłaszcza w zakresie cyberprzestępstw skróciłby się nawet dwukrotnie, a cele postępowania przygotowawczego mogłyby zostać osiągnięte w maksymalnym z postulowanych zasad stopniu. Wyrazić jednak należy ogromną nadzieję, że analiza rynków światowych, otaczającej nas sytuacji, nieustannego postępu technologicznego oraz nieprawdopodobnie dynamicznego wzrostu popularności tego rodzaju usług zmusi prawodawcę do refleksji i być może sprawi, że polskie ustawodawstwo, polski porządek prawny, a w konsekwencji system pracy zwłaszcza zawodów prawniczych będzie jeszcze bliżej nowych technologii.

3. Postulaty z punktu widzenia innych zawodów prawniczych

Nie ma wątpliwości co do tego, iż zmiany i udoskonalenia są niezbędne nie tylko w odniesieniu do profesji organów ścigania, ale również w przypadku pozostałych zawodów prawniczych. Potrzebę informatyzacji i szerszego wprowadzenia nowych technologii dostrzega się w większości zawodów, zwłaszcza w tych, które cenią sobie komfort pracy i jej efektywność jak również otwartość na zmiany oraz podążanie za rozwijającym się postępem technologicznym. W związku z tym coraz częściej dostrzega się obecność dokumentów cyfrowych zamiast papierowych – tradycyjnych. Aktualna sytuacja na rynku wskazuje, iż te zawody, które skutecznie przeprowadziły transformację cyfrową, osiągają cele i rezultaty na o wiele wyższym poziomie aniżeli te same usługi korzystające nadal z tradycyjnych metod

obrotu dokumentów i danych. Nie ma wątpliwości co do tego, iż praca w oparciu o dokumenty cyfrowe jest bardziej ekonomiczna z wielu punktów widzenia – czasu, miejsca, a niekiedy również nakładu finansowego.

Wśród profesji prawniczych, zwłaszcza wolnych zawodów coraz bardziej popularne staje się wykorzystanie nowych technologii w praktyce, a także podjęcie LegalTech. Pojęcie LegalTech pochodzi od połączenia dwóch słów, tj. „Legal", które w tłumaczeniu oznacza prawny, prawniczy oraz „Tech" jako skrótu słowa „*technology*", które oznacza technologię. LegalTech są to zatem narzędzia informatyczne optymalizujące prace związane ze stosowaniem prawa. Pozwalają na automatyzację i informatyzację tworzenia dokumentów prawnych, wyszukiwanie, analizę i zarządzanie informacjami (*legal research*), obsługę klientów oraz dostęp, integrację i przechowywanie danych. Okoliczności pandemii i związanej z nią transformacji mającej na celu ograniczenie kontaktów bezpośrednich, przyśpieszyły także wprowadzenie doręczeń elektronicznych dokonywanych za pośrednictwem Portalu Informacyjnego Sądów Powszechnych. Katalog narzędzi LegalTech jest bardzo szeroki, zalicza się do niego przede wszystkim różne oprogramowania, w tym programy przeznaczone do edycji tekstu takie jak Word, ale również bardziej skomplikowane narzędzia w postaci programów wykorzystujących działanie chociażby sztucznej inteligencji. Adwokatura dostrzega konieczność przyjęcia jednolitych wytycznych dla ochrony bezpieczeństwa korzystania z technologicznych rozwiązań. Instytut LegalTech Naczelnej Rady Adwokackiej sukcesywnie pracuje nad przygotowaniem standardów cyberbezpieczeństwa dla adwokatów, które pozwolą na wdrożenie odpowiednich praktyk i procedur bezpieczeństwa, niezwykle istotnych dla ochrony tajemnicy adwokackiej.

W zakresie tzw. merytorycznej pracy adwokatów czy radców prawnych w zasadzie ciężko postulować o „uniwersalne" rozwiązania, albowiem każdy przyjmuje inne metody rozmawiania z klientami, korespondowania z nimi, warunki generowania umów czy udzielania szeroko rozumianych porad prawnych. Nie ma wątpliwości co do tego, iż działanie nowych technologii bez wątpienia może przyczynić się do wzrostu wydajności pracy prawników w tym zakresie, skrócenia czasu ich pracy, a także jej ułatwienia, niemniej jednak sformułowanie postulatów w zakresie uregulowania pewnych jednolitych rozwiązań jest w zasadzie niemożliwe w tym zakresie. Oprócz sfery dotyczącej typowo merytorycznej pracy z klientami, w profesji prawników wyróżnić można tzw. sferę organizacyjno-administracyjną, czyli taką która de facto nie jest stricte związana z merytorycznym udzieleniem porad prawnych oraz analizą przepisów, a dotyczy sposobu wymiany korespondencji z klientem,

ewidencjonowaniem czasu pracy, rozliczaniem swojej działalności, wystawianiem faktur itp. O ile w przypadku wymiany korespondencji z klientem oraz przesyłania projektów pism procesowych celem zatwierdzenia wykorzystuje się najczęściej drogę elektroniczną, zaś dla generowania faktur i ich rozliczania w bardzo łatwy sposób można wykupić przeznaczone do tego intuicyjne oprogramowanie, o tyle w pozostałym zakresie brak jest jakichkolwiek narzędzi, które ułatwiłyby tą pracę.

Jak wskazują badania przeprowadzone w 2017 r. wśród prawników najczęściej krytykowaną kwestią jest brak narzędzia czy oprogramowania, które ułatwiłoby i skróciło czas realizacji tzw. czynności administracyjnych polegających na ewidencjonowaniu czasu pracy i obliczaniu kosztów wynagrodzenia. Zdecydowana większość adwokatów i radców prawnych ma kłopot z jednoznacznym ustaleniem wysokości stawki za wykonanie szeroko rozumianej pomocy prawnej dla konkretnego klienta. Czas, który aktualnie poświęcany jest na przygotowanie rzeczonych czynności mógłby zostać wykorzystany dla bardziej skrupulatne przygotowanie pisma procesowego, przygotowanie reklamy czy pozyskanie nowego klienta. Odpowiedzią na głośno wybrzmiewającą krytykę w tym zakresie byłoby opracowanie specjalnie przygotowanego oprogramowania, dostępnego wyłącznie dla prawników i dostosowanego stricte do potrzeb ich profesji. W praktyce takie oprogramowanie oczywiście niestety musiałoby być odpłatne, niemniej jednak baza korzyści zdecydowanie przewyższałaby ewentualną wartość kosztów. Wśród narzędzi, jakie udostępniałoby takie programowanie byłaby możliwość tworzenia katalogów odrębnych dla każdego konkretnego klienta, w ramach którego możliwe byłoby ewidencjonowanie nakładu pracy wymaganego w konkretnym przypadku z podziałem na sporządzanie pism procesowych, ewentualne pobyty w sądzie, rozmowy z klientem – osobiste i telefoniczne, konieczność zapoznania się z aktualnymi przepisami prawnymi i orzecznictwem. Na tej podstawie system umożliwiałby wyliczenie szacunkowych kosztów wynagrodzenia za udzieloną pomoc prawną, przy uwzględnieniu wszystkich wyżej wymienionych czynników. Algorytm w tym zakresie musiałby być odpowiednio opracowany, z właściwym uwzględnieniem uregulowań wynikających z właściwych rozporządzeń, a także przyznaniem właściwej wagi dla najistotniejszych i najbardziej pracochłonnych – a w konsekwencji „najdroższych" etapów pracy prawnika. Stworzenie systemu dot. ewidencjonowania czasu pracy oraz program umożliwiający szacunkowe wyliczenie wynagrodzenia za wykonaną pracę, opracowany na podstawie algorytmu uwzględniającego odczytany z systemu zewidencjonowany czas pracy, ilość napisanych pism procesowych, ewentualnie udziału w rozprawach, spotkania z klientami –

pozwoli to na wyrównanie wynagrodzeń na rynku i zniwelowanie różnic – oczywiście pozostawiając margines na swobodną ocenę prawnika.

Oczywiście nie sposób wymagać od oprogramowania dokładnego wyliczenia stawki wynagrodzenia, albowiem należy również uwzględnić możliwość samodzielnego regulowania ostatecznej ceny, niemniej jednak nie ma wątpliwości, że takie narzędzie w sposób znaczny ułatwiłoby w wielu przypadkach wycenę usług prawniczych. System taki pozwoliłby nadto na ewidencjonowanie wszelkich organizacyjnych kwestii dotyczących klientów, pozwalając na przechowywanie informacji w jednym miejscu, przy czym w przypadku stałych klientów ewidencjonować można byłoby również kwestię rozliczeń, unikając w ten sposób problemów w tej sferze. Reasumując wskazaną kwestię, nie ma w zasadzie wątpliwości co do tego, że oprogramowanie wykorzystujące działanie nowych technologii w sposób znaczny przyczyniłoby się do ułatwienia wskazanej sfery działalności adwokatów i radców prawnych, wywierając tym samym bezpośredni wpływ na jakość oferowanych przez nich usług.

Jak się okazuje, nowe technologie i inwestowanie w usługi związane bezpośrednio z tą sferą odgrywają istotną rolę w szeroko rozumianej branży prawniczej. O ile często spotyka się prawników, którzy twierdzą, iż nie potrzebują w związku z prowadzoną przez siebie działalnością gospodarczą rozwiązań technologicznych, o tyle zdecydowanie częściej na rynku spotyka się prawników świadomych postępu technologicznego i plusów z niego wynikających, przy okazji ich wykorzystania[377]. Praktyka wskazuje, iż potrzeby coraz to nowszych rozwiązań technologicznych prawnicy poszukują najczęściej w sferach organizacyjnych i administracyjnych, uważając, że w pracy merytorycznej niezawodne i pewne pozostają tradycyjne metody. W ocenie prawników celem wprowadzenia do ich profesji rozwiązań i narzędzi wykorzystujących działanie nowych technologii, w tym również sztucznej inteligencji jest przede wszystkim usprawnienie wielu obszarów ich działań, informatyzacja podstawowych i rutynowych czynności, minimalizacja nakładu pracy na kwestie administracyjne.

Jak na wstępie wskazano, potrzeba pewnych przeobrażeń dostrzegalna jest również w przypadku pozostałych zawodów prawniczych. W związku z tym, iż przedmiotowa praca oraz prowadzone na jej kanwie badania i uzyskane w ten sposób wyniki w znacznym stopniu dotyczyły profesji organów ścigania, zwłaszcza prokuratury, poniżej przedstawione zostaną

[377] https://legaltechpolska.pl/wp-content/uploads/2018/06/2018.06.25_Raport_LegalTech_ost.pdf (dostęp: 06.06.2023 r.)

najistotniejsze postulaty, których potrzebę ujawniono podczas prowadzenia badań. Postulaty te w głównej mierze dotyczyć będą szeroko rozumianej współpracy organów ścigania z wolnymi zawodami. W sposób jednoznaczny stwierdzić należy, iż rzeczona współpraca jest w zasadzie codziennością, a jej prawidłowy przebieg leży w interesie obu stron, albowiem każdy ma interes z odpowiednim zakończeniu postępowania przygotowawczego – pomimo, iż interesy te niejednokrotnie bywają rozbieżne, aczkolwiek czas i możliwość najszybszego zakończenia śledztwa lub dochodzenia co do zasady są tożsame.

Adwokat lub radca prawny reprezentujący daną stronę postępowania przygotowawczego, występując w charakterze pełnomocnika pokrzywdzonego albo obrońcy oskarżonego, zazwyczaj pierwszy kontakt z organami ścigania (przy przyjęciu, iż wstępuje do już toczącego się postępowania przygotowawczego, a nie je inicjuje) ma miejsce w przypadku potrzeby wglądu w akta sprawy. Nie ma wątpliwości co do tego, iż przebieg prawidłowego stosunku obrończego czy reprezentacji pokrzywdzonego w dużej mierze uzależniony jest od wiedzy profesjonalnego pełnomocnika o etapie postępowania przygotowawczego, dotychczas poczynionych ustaleniach i zgromadzonym materiale dowodowym, albowiem fakty te bezpośrednio determinują przyjęcie określonej linii obrony. Zgodnie z obowiązującymi przepisami ww. osoby mają prawo wglądu do akt postępowania, po uprzednim wykazaniu pełnomocnictwa lub jego uwierzytelnionej kopii. Praktyka wskazuje, iż adwokat lub radca prawny w tym celu składa do prokuratora nadzorującego dane postępowanie pisemny wniosek o wgląd w akta sprawy, następnie ustalają odpowiedni termin na przeprowadzenie tej czynności, a dopiero wówczas jawi się możliwość faktycznego przejrzenia akt postępowania przygotowawczego. Niejednokrotnie czas oczekiwania na przedmiotową czynność znacznie się wydłuża, albowiem normalną procedurą jest to, że w celu przeprowadzenia danego postępowania i zgromadzenia materiału dowodowego akta główne przekazywane są na Policję. Dopiero po ich ponownym przyjęciu do właściwej jednostki prokuratury, możliwe jest wykonanie opisywanej czynności. Okoliczności te są bezpośrednią przyczyną głośno pojawiającej się krytyki w tym zakresie, zwłaszcza po stronie wolnych zawodów, które coraz częściej domagają się digitalizacji akt postępowania przygotowawczego, co w sposób zdecydowany ułatwiłoby organizację ich pracy i skuteczne prowadzenie zleconej sprawy.

Generalnie przyjmuje się, iż digitalizacja polega na przeobrażeniu dokumentów w wersji papierowej w dokumenty elektroniczne, czyli pliki cyfrowe przy pomocy najczęściej urządzeń skanujących. Pomysł digitalizacji akt przyjął się już w części jednostek prokuratur na terenie kraju, zwłaszcza w jednostkach wyższego rzędu, które obecnie dysponują w większości

materiałami w wersji elektronicznej. W drugiej połowie 2022 r. wdrożono polecenie Prokuratury Krajowej dotyczące digitalizacji akt postępowania przygotowawczego w pierwszej kolejności dotyczących postępowań, w których zastosowano środek zapobiegawczy w postaci tymczasowego aresztowania, prowadzonych w formie śledztw oraz zakończonych aktem oskarżenia do sądu. Pomimo skierowania takiego polecenia, nie wszystkie jednostki wdrożyły ten element, co w zdecydowanej większości spowodowane jest brakami kadrowymi oraz bezwzględną koniecznością zatrudnienia osób, które odbędą szkolenie z zakresu digitalizacji akt i ich praca będzie stricte dotyczyła tej kwestii. Wyłącznie takie rozwiązanie umożliwi pełną digitalizację wszystkich akt postępowań przygotowawczych, bez uszczerbku dla merytorycznej pracy pozostałych pracowników oraz kwestii organizacyjnej całej jednostki. O ile postulat digitalizacji akt postępowania przygotowawczego zdaje się być w pewnym aspekcie negatywnym zjawiskiem dla organów ścigania, albowiem nakłada na nich dodatkowe obowiązki w postaci transformacji tradycyjnych materiałów postępowania do wersji dokumentów elektronicznych, o tyle bez wątpienia stwierdzić należy, iż w przyszłości przyniesie to zdecydowanie więcej korzyści aniżeli faktycznych ewentualnych trudności.

Pełna digitalizacja akt postępowania przygotowawczego bez wątpienia byłaby nieprawdopodobnie korzystnym rozwiązaniem z punktu widzenia wolnych zawodów, które dzięki temu uzyskałyby możliwość w zasadzie nieograniczonego czasowo i miejscowo wglądu w akta interesującej ich sprawy. Formalne zorganizowanie tej kwestii nie jest skomplikowanym procesem i należałoby go opracować w sposób analogiczny jak aktualnie funkcjonuje portal sądowy, umożlwiający wgląd do wszelkich orzeczeń wydawanych w toku danej sprawy na etapie postępowania sądowego. W związku z tym niezbędne byłoby posiadanie przez profesjonalnych pełnomocników zarejestrowanych kont na odpowiednio przygotowanym portalu zorganizowanym na podobieństwo powyższego, a następnie skierowaniu do odpowiedniej prokuratury w wersji elektronicznej wniosku o wgląd w akta sprawy. Wniosek po pozytywnym rozpoznaniu umożliwiłby profesjonalnym pełnomocnikom wgląd w materiały postępowania w wersji dokumentów elektronicznych na odległość, w zasadzie w każdym czasie i na każdym etapie postępowania przygotowawczego – oczywiście do czasu posiadania odpowiedniego umocowania i legitymacji do występowania w procesie. Cała ta procedura pozytywnie wpłynęłaby na współpracę wskazanych zawodów prawniczych, w sposób znaczny skracając czas komunikacji, umożliwiając z kolei szersze wykorzystanie nowych technologii wśród zawodów prawniczych.

Niemniej jednak, perspektywa pełnej digitalizacji akt postępowania przygotowawczego zdaje się być bardzo obiecująca, albowiem pojawia się w wielu zaleceniach Prokuratury Krajowej, która z pewnością w niedalekiej przyszłości zacznie domagać się wprowadzenia tej transformacji w życie w pełnym jej wymiarze.

Przy okazji omawiania postulatów dotyczących pozostałych zawodów prawniczych, tzn. innych niż organy ścigania przypomnieć należy również o kwestii, o której wspominano na kanwie rozdziału dotyczącego komunikacji elektronicznej wykorzystywanej przez wolne zawody. Nie ma żadnych wątpliwości co do tego, iż aktualnie głównym sposobem komunikacji, nie tylko wśród zawodów prawniczych, jest komunikacja elektroniczna za pośrednictwem poczty elektronicznej czyli potocznie zwanych maili. Obecnie adwokaci i radcy prawni komunikują się w kwestiach zawodowych, w tym zarówno z klientami, jak również organami ścigania za pośrednictwem zarejestrowanych na siebie adresów poczty elektronicznej. Przeprowadzone badania wskazują, iż w zdecydowanej większości przedstawiciele wolnych zawodów korzystają z bezpłatnych, ogólnodostępnych domen internetowych, gdzie zdecydowanie dominującą jest domena gmail.com, administrowana przez Google. Zdarzają się również przypadki, w których wykorzystywane są domeny obsługiwane przez polskie podmioty, takie jak Grupa Wirtualna Polska S.A., czy Grupa Onet.pl lub Interia.pl. Zdecydowanie rzadziej dostrzega się adresy poczty elektronicznej zarejestrowane na płatnych, zindywidualizowanych domenach. Reasumując, w zdecydowanej większości mamy do czynienia z bezpłatnymi adresami mailowymi, które w zasadzie korzystają z minimalnej ochrony, pomimo przesyłania za ich pośrednictwem niezwykle ważnych, poufnych dokumentów i informacji. Aktualnie obowiązujące regulacje prawne nie nakładają na zawody prawnicze obowiązku posiadania adresów mailowych na konkretnych domenach, z odpowiednim poziomem bezpieczeństwa, co należy ocenić bardzo krytycznie. Analiza sposobu popełniania cyberprzestępstw na terenie kraju wskazuje, iż nawet kilkanaście procent z nich popełnianych jest przy wykorzystaniu narzędzia komunikacji elektronicznej jakim jest adres mailowy. Sprawca uzyskując dostęp do skrzynki elektronicznej w zasadzie uzyskuje dostęp do całości korespondencji prowadzonej za jej pośrednictwem, co okazuje się być nieprawdopodobnie niebezpieczne z punktu widzenia uzyskania danych przez osoby nieuprawnione. Kwestia ta w sposób bezpośredni wskazuje, iż skrzynki mailowe, również prawników, mogą stać się przedmiotem cyberataków.

Pomimo ogromnego postępu w zakresie komunikacji wśród zawodów prawniczych, ustawodawca nie przewidział narzędzi, które w sposób możliwie maksymalny zapewniłyby

bezpieczeństwo przekazywanych danych. Nie ma wątpliwości co do tego, że skoro komunikacja elektroniczna aktualnie jest na bardzo zaawansowanym poziomie, niezbędne jest przyjęcie regulacji, które zapobiegną ewentualnym niebezpieczeństwem związanym z komunikacją na odległość. Stwierdzić zatem należy, iż w pełni celowe i uzasadnione zwłaszcza z punktu widzenia postępu technologicznego, jest wprowadzenie oraz przyjęcie takich rozwiązań prawnych, które będą nakładać na wolne zawody obowiązek posiadania adresów poczty elektronicznej na konkretnych domenach, prowadzonych przez właściwy podmiot. W tym celu niezbędne byłoby oczywiście przygotowanie i odpowiednie zabezpieczenie takiej domeny, a w konsekwencji zarejestrowanych kont. Współpraca pomiędzy izbami adwokatów i radców prawnym w tym aspekcie byłby bardzo znacząca. Konieczne byłoby zastosowanie narzędzi, które zapewniłby najwyższy z możliwych poziomów bezpieczeństwa, na podobieństwo chociażby obecnie obowiązujących wewnętrznych adresów mailowych w jednostkach państwowych. Wyłącznie takie rozwiązanie pozwoliłoby na faktycznie skutecznie korzystanie z narzędzi jakie udostępniają nowe technologie, przy jednoczesnym zapewnieniu ochrony informacji i dokumentów, jakie przesyłane są za pośrednictwem komunikacji elektronicznej. Praktyka wskazuje, iż stanowisko postulujące takie rozwiązanie staje się coraz bardziej popularne również wśród zawodów prawniczych, które również dostrzegają potrzebę zapewnienia większej ochrony przesyłanych treści. Niemniej jednak wciąż najbardziej popularne są darmowe skrzynki pocztowe, niestety zapewniające minimalne bezpieczeństwo przesyłanych i przechowywanych danych.

Reasumując poczynione w tym zakresie ustalenia, wskazać należy, iż potencjał nowych technologii zdaje się być bardzo obiecujący, istotą jest możliwość skorzystania z jego możliwości. Udostępnienie przez prawodawcę narzędzi w tym zakresie, zwłaszcza dla organów ścigania, staje się idealnym środkiem umożliwiającym maksymalizację celów postępowania karnego, to jest jego przyspieszenia, a w konsekwencji zwiększa szansę na wykrycie sprawcy przestępstw i pociągnięcie go do odpowiedzialności. Jak wyżej wskazano, profesja organów ściągania, nie jest jedyną wśród zawodów prawniczych, wymagającą modernizacji i informatyzacji, niemniej jednak sukcesywnie wdrażane są rozwiązania innowacyjne, które należy ocenić pozytywnie i z nadzieją oczekiwać na ich coraz większy stopień zaawansowania.

Zakończenie

Przeprowadzone na tle niniejszej rozprawy kompleksowe badania w zakresie wpływu nowych technologii na funkcjonowanie zawodów prawniczych, w sposób jednoznaczny i zupełny potwierdziły wskazaną na wstępie główną tezę, zgodnie z którą postęp technologiczny wywołuje bezpośredni wpływ na funkcjonowanie zawodów prawniczych, powodując możliwość wyodrębnienia nie tylko pozytywnych jego następstw, ale również wskazania negatywnych czynników wynikających wprost z nieustannego rozwoju technologicznego. Przywołane stanowisko determinuje konieczność sformułowania niejako następczych wniosków *stricte* związanych z innowacyjnymi narzędziami, a w odniesieniu do których problemy badawcze ujawniły się również w trakcie prowadzonych badań.

Rozwój technologiczny odnosi nieprawdopodobnie znaczący wpływ na wiele dziedzin życia społecznego, niemniej jednak kwestia ta nie stanowiła najistotniejszego aspektu na tle czynionych rozważań, albowiem w zasadzie nie budzi ona wątpliwości. Niemniej jednak, problemem badawczym podjętym i rozwiązanym przez autora na gruncie niniejszej rozprawy, była przede wszystkim ocena wpływu nowych technologii na funkcjonowanie zawodów prawniczych, w odniesieniu do każdej grupy zawodowej, a także ocena stopnia i charakteru tego wpływu, przy jednoczesnym omówieniu faktycznego wykorzystywania potencjału nowych technologii. W zdecydowanej większości rozważania dotyczyły profesji organów ścigania, z uwagi na ścisły związek autora z tą grupą zawodową oraz możliwość sformułowania wniosków w wymiarze praktycznym, a jednocześnie pośrednio wdrożeniowym.

W pierwszej kolejności wskazać należy, iż przeprowadzone badania wprost dowodzą, że wszystkie zawody prawnicze, w mniejszym lub większym stopniu wykorzystują w swojej pracy narzędzia związane bezpośrednio z nowymi technologiami, które sukcesywnie ulegają udoskonaleniu na przestrzeni czasów i wprowadzanych w tym zakresie zmian. Z uwagi na charakter tej grupy zawodowej, wprowadzenie wielu rozwiązań jest niemożliwe lub znacznie utrudnione, co podyktowane jest koniecznością zapewnienia maksymalnych standardów bezpieczeństwa, zwłaszcza w zakresie przetwarzanych informacji i zapewnienia odpowiedniej ochrony danych. Niemniej jednak, nie ulega wątpliwości, iż nowe technologie sukcesywnie udoskonalane na płaszczyźnie funkcjonowania zawodów prawniczych, w sposób zdecydowany wpłynęły na sposób realizowania ich zadań, ale również na komfort pracy. Tak jak każda zmiana powoduje ujawnienie zarówno pozytywnych jak i negatywnych jej następstw, tak również analogiczne zjawisko możliwe jest do wykazania w przypadku zmian dokonywanych

w szeroko rozumianym obrocie prawnym na skutek nieustających i nieuchronnych zmian technologicznych. Nie ma wątpliwości co do tego, iż postęp technologiczny dostarcza zawodom prawniczym, a zwłaszcza organom ścigania, narzędzi innowacyjnych, które w konsekwencji przekładają się nie tylko na jakość realizowanych zadań, ale również na maksymalizację celów pracy konkretnej grupy zawodowej. Wprowadzenie do pracy organów ścigania instrumentów funkcjonujących w zdecydowanej większości w oparciu o sieć teleinformatyczną, w szczególności udostępnienie prokuratorom dostępu do baz danych umożliwiających identyfikację szerokiego katalogu okoliczności, bez wątpienia usprawniło pracę tej grupy zawodowej. Ocena pracy organów ścigania rozpatrywana przez pryzmat wykorzystania nowych technologii na przestrzeni ostatnich 3 lat uległa znacznej informatyzacji i modernizacji, o czym świadczy przede wszystkim fakt udostępnienia dla tej grupy zawodowej dedykowanego systemu teleinformatycznego o nazwie ProkSys, w ramach którego udostępniono wiele rozwiązań determinujących szybkość i sposób realizacji zadań prokuratora i pracowników prokuratury, zwłaszcza w zakresie procesowego zabezpieczenia danych telekomunikacyjnych oraz bezpośredniego dostępu do kluczowych baz danych.

Niewątpliwym i jednocześnie bardzo doniosłym aspektem bezapelacyjnie wynikającym z postępu technologicznego i jego pośredniego wpływu na funkcjonowanie zawodów prawniczych, jest kwestia cyberprzestępczości. Aktualnie, cyberprzestępstwa, czyli czyny zabronione popełniane za pośrednictwem sieci teleinformatycznej, stanowią największą liczbę przestępstw popełnianych na terenie kraju. Wśród czynników powodujących to zjawisko, najogólniej rzecz ujmując wskazać należy rozwój technologiczny, który bezpośrednio wpływa na okoliczności determinujące nieustanny wzrost przestępczości w tym zakresie. Precyzując postawioną tezę podkreślenia wymaga przede wszystkim fakt, iż aktualnie otaczająca nas rzeczywistość, w której większość usług realizowanych jest za pośrednictwem sieci teleinformatycznej, a komunikacja elektroniczna jest dominującym środkiem łączności, a także gdzie odnotowywany jest sukcesywny wzrost zainteresowania portalami społecznościowymi, stała się doskonałym środowiskiem dla sprawców cyberprzestępstw. Udostępnianie coraz to nowszych, bardziej doskonałych narzędzi technologicznych pośrednio umożlwiających popełnianie czynów zabronionych za pośrednictwem sieci teleinformatycznej, sprawia, iż sprawcy przejawiają poczucie złudnej anonimowości, co z kolei składnia ich do popełniania większej liczby cyberprzestępstw. Nadto kwestie ekonomiczne, pozwalające na uzyskanie w sposób przestępczy znaczących sum pieniężnych, również stają się zachętą dla przestępców. Okoliczności te wprost dowodzą, iż poza niekwestionowanie pozytywnymi aspektami nowych

technologii, wyróżnić można również ich negatywne oblicze, przejawiające się na potężną skalę cyberprzestępczości. Jak wskazują wyniki przeprowadzonych na kanwie przedmiotowej pracy badań, rozwój technologiczny bezpośrednio spowodował powstanie narzędzi, które ułatwiają, a niekiedy umożliwiają sprawcom przestępcze działanie. Wśród takich czynników wyróżnić można przede wszystkim maskowanie ruchu w sieci internetowej, różnego rodzaju techniki manipulacyjne o charakterze socjotechnicznym, które w sposób gwałtowny wpływają na zachowanie potencjalnych pokrzywdzonych. Możliwość działania na odległość, z pozycji jakiegokolwiek urządzenia umożliwiające komunikację elektroniczną, niejednokrotnie z innego kraju aniżeli miejsce pobytu pokrzywdzonego, to kolejne czynniki stanowiące aspekty zachęcające sprawców do karygodnego i przestępczego działania. Przytoczone okoliczności potwierdza nadto fakt, iż pierwotnie sposób działania sprawców cyberprzestępstw był bardzo podstawowy, natomiast na skutek rozwoju nowych technologii zaczęły funkcjonować coraz bardziej zaawansowane struktury przestępcze oraz coraz bardziej doskonałe metody sprawcze, które w konsekwencji w sposób znaczny utrudniały lub nawet uniemożliwiały wykrycie sprawców przez organy ściągania. Nadto pojawiające się na przestrzeni lat nowe instrumenty zachęcające pokrzywdzonych np. do zainwestowania środków finansowych za pośrednictwem internetu, w tym platformy inwestycyjne, giełdy finansowe związane z obrotem kryptowalutami powodują, iż na tej płaszczyźnie odnotowywanych jest aktualnie najwięcej przestępczych działań.

Wyżej przytoczone okoliczności wprost wskazują na znaczny wpływ nowych technologii na funkcjonowanie zawodów prawniczych, w tym przypadku na organy ścigania, których praca niejako zostaje w tym aspekcie determinowana przez sposób działania sprawców cyberprzestępstw. Nie ulega wątpliwości, iż każdorazowy wybór metody wykrywczej przyjętej przez organy ścigania podyktowany jest rodzajem przestępstwa stanowiącego przedmiot postępowania przygotowawczego. Analogicznie kwestia ta wygląda w przypadku przestępstw popełnianych za pośrednictwem sieci teleinformatycznej. Nadto sposób działania sprawców determinuje konieczność wyodrębnienia wielu rodzajów cyberprzestępstw, co również odnosi bezpośredni wpływ na wybór metody mającej na celu wykrycie, a następnie pociągnięcie do odpowiedzialności karnej sprawcy przestępstwa. Na tle przedmiotowej rozprawy w sposób precyzyjny omówiono sposoby działania organów ścigania w przypadku postępowań przygotowawczych prowadzonych o przestępstwa internetowe, wśród których zdecydowanie dominują oszustwa, czyli przestępstwa stypizowane w art. 286 § 1 kodeksu karnego. Mając to na względzie, wskazać należy, iż organy ścigania każdorazowo opracowują niejako odpowiedź

dla cybersprawców z w postaci sukcesywnie przygotowywanych i dopracowywanych algorytmów procesu wykrywczego, w którym wykorzystują innowacyjne narzędzia, a także poprzez organizowanie zespołów do walki z cyberprzestępczością (co do zasady na szczeblu Prokuratur Okręgowych) a także szkoleń związanych *stricte* z konkretnymi rodzajami przestępstw. Algorytmy wykrywcze organów ścigania stanowią pewien schemat działania, którego głównym celem jest ustalenie tożsamości sprawcy cyberprzestępstw. W związku z tym, iż w przypadku tego rodzajów czynów zabronionych dominującą siłą napędową i wykorzystywanymi narzędziami są rozwiązania innowacyjne, algorytmy muszą być przygotowane w taki sposób, aby podążać za tą innowacyjnością, w związku z czym dominującą ich część stanowi zabezpieczenie danych telekomunikacyjnych zwanych retencyjnymi, a następnie analiza tych danych za pośrednictwem narzędzi opartych o działanie sieci teleinformatycznej, które są udostępniane organom ścigania.

Pomimo sukcesywnego doskonalenia procesu wykrywczego, udostępnianie coraz to bardziej zaawansowanych narzędzi, wstąpienie w szeregi organów ścigania wyspecjalizowanych w tym zakresie osób, nieustannie prowadzone szkolenia w tym zakresie, fakt regularnego ulepszania metod przestępczych, wykorzystywania technik maskujących ruch w sieci sprawia, iż wykrywalność przestępstw tego rodzaju przedstawia się na niskim poziomie, a główną przyczyną zakończenia tego rodzaju postępowań przygotowawczych jest niewykrycie sprawcy czynu zabronionego (art. 322 § 1 kodeksu postępowania karnego). Niezależnie od powyższego, nieustannie rosnąca świadomość cyberzagrożeń wśród społeczeństwa, coraz większe wykorzystanie potencjału nowych technologii przez ograny ścigania, wprowadzenie do ich pracy coraz to bardziej zaawansowanych narzędzi sprawia, iż istnieje duże prawdopodobieństwo zdecydowanego zminimalizowania liczby przestępstw tego rodzaju. Cyberbezpieczeństwo stanowi niewątpliwie ujemną konsekwencję nowych technologii, niemniej jednak istnieje wiele czynników pozwalających na przypisanie pozytywnego wpływu na zawody prawnicze. Kwestia ta różni się w zależności od grupy zawodowej, a na przestrzeni przedmiotowej pracy przedstawiono szeroki katalog narzędzi wykorzystywanych przez każdą z grup zawodowych.

Poza badaniami prowadzonymi w zakresie wpływu nowych technologii na funkcjonowanie zawodów prawniczych, a w konsekwencji podjętej analizy prawnokarnej odnoszącej się do cyberprzestępczości, podjęto próby rozwiązania problemu badawczego odnoszącego się do statusu społeczeństwa polskiego rozpatrywanego przez status jego informacyjności. Przeprowadzone w tym aspekcie badania ilościowe wśród bardzo

zróżnicowanej grupy badawczej dostarczyły znaczących z perspektywy nauk społecznych wniosków. Kategorycznego zaznaczenia wymaga fakt, iż obecnie funkcjonujące społeczeństwo stanowi bardzo zaawansowane stadium społeczeństwa informacyjnego, w którym zdecydowana część zarówno pozyskania jak i wymiany informacji odbywa się za pomocą środków komunikacji elektronicznej. W społeczeństwie, komunikacja z innymi ludźmi odbywa się w zdecydowanej większości przypadków za pośrednictwem komunikacji na odległość, a usługi użyteczności publicznej oferowane w sieci teleinformatycznej wykorzystywane są na wysokim poziomie w społeczeństwie. Struktura sieci teleinformatycznej, sposób jej rozbudowania, swobodna możliwość wyboru spośród wielu operatorów sieci komórkowej oraz dostawców internetu, sprawia, iż społeczeństwo informacyjne funkcjonuje w oparciu o zaawansowane standardy umożlwiające w ogóle jego przyjęcie. Nieustannie rosnące zainteresowanie i popularność portalami społecznościowymi oraz komunikatorami społecznościowymi powoduje, iż są to przeważające źródła łączności, wymiany informacji, codziennej komunikacji, ale również innych usług, takich jak chociażby zakupy przez Internet. Uzyskane wyniki badań spowodowały konieczność podjęcia próby sformułowania definicji rodzaju społeczeństwa informacyjnego, które zdecydowanie bardziej odzwierciedla jego aktualną strukturę i cechy, tj. społeczeństwa sieci rozumianego jako szczególny rodzaj społeczeństwa informacyjnego, w którym najistotniejszym czynnikiem jest w zasadzie nieograniczony dostęp do sieci teleinformatycznej, a w którym podstawowym sposobem komunikacji jest komunikacja elektroniczna.

Bezapelacyjnie kwestią ściśle związaną z nowymi technologiami i ich rozwojem jest aktualnie ulegająca znacznej popularyzacji sztuczna inteligencja stanowiąca przyszłość wielu zawodów oraz obietnicę udoskonalenia wielu aspektów życia za pomocą urządzeń wykorzystujących jej potencjał. W mediach coraz częściej prezentowane jest stanowisko, zgodnie z treścią którego sztuczna inteligencja stanowi bezpośrednie zagrożenie dla zawodów prawniczych i istnieje poważne ryzyko ich zastąpienia właśnie przez mechanizmy sztucznej inteligencji. Przeprowadzone badania jednakże wprost wskazują na konieczność ostudzenia emocji wynikających z prezentowanych i ferowanych przez media takich stanowisk. Nie ulega wątpliwości, że rozwiązania wykorzystujące potencjał sztucznej inteligencji są jak najbardziej pożądane wśród wszystkich zawodów prawniczych. Postulat maksymalnego przyspieszenia i ułatwienia wszelkich możliwych formalności, bezpośrednio pociąga za sobą potrzebę zautomatyzowania pewnych czynności procesowych, zwłaszcza przy wykorzystaniu uczenia maszynowego. Niemniej jednak dotyczy to wprost kwestii wsparcia tej grupy zawodowej oraz

pomocniczego wykorzystania algorytmu sztucznej inteligencji, nie zaś jakiejkolwiek możliwości całkowitego zastąpienia tej grupy zawodowej, co w ocenie autora jawi się jako niemożliwe. Za słusznością tego stanowiska przemawia przede wszystkim charakter tej grupy zawodowej oraz charakter realizowanych czynności. W odniesieniu do grupy wolnych zawodów jednoznacznego podkreślenia wymaga fakt, iż działanie tej grupy zawodowej bez wątpienia oparty jest o kwestię zaufania, która stanowi fundament współpracy z klientem, a co jest niemożliwe do osiągnięcia przez algorytm sztucznej inteligencji. Co więcej, praca prawników oparta jest na logicznym myśleniu, wymagającym niejednokrotnie nagłej modyfikacji przyjętej strategii działania na skutek zmiany sytuacji procesowej, co również jest trudne do wyobrażenia w przypadku sztucznej inteligencji. W przypadku organów ścigania, ze względu na szczególną specyfikę tej branży oraz wymóg zapewnienia najwyższych standardów bezpieczeństwa, uznać należy, iż nie jest to środowisko, w którym można ryzykować wprowadzeniem eksperymentalnych rozwiązań w zakresie sztucznej inteligencji. Powyżej przytoczone tezy nie oznaczają jednakże, iż grupa prawników powinna być w pełni zamknięta na rozwiązania oparte o proces maszynowego uczenia się, albowiem bez wątpienia sztuczna inteligencja wyposażona jest w nieprawdopodobny potencjał mogący usprawnić i udoskonalić pracę tej grupy zawodowej. Przy okazji futurologicznego rozstrzygania kwestii umożliwiających wprowadzenie sztucznej inteligencji, wyraźnie zaznaczyć należy, iż odbywa się to wyłącznie w kategorii hipotetyzowania, albowiem przyjęcie uczenia maszynowego wśród zawodów prawniczych, zwłaszcza w przypadku pracy organów ścigania i wymiaru sprawiedliwości nie jest zasadniczo prostym zabiegiem. Niezależnie od powyższego sztucznej inteligencji nie należy ignorować, jest to bowiem mechanizm, który na skutek rozwoju technologicznego, może zostać wykorzystany przez cyberprzestępców na bardzo szeroką skalę. W środowisku prawniczym słusznie się wskazuje, iż ww. sprawcy mają w ten sposób możliwość niejako zautomatyzowania swoich ataków.

Badania w zakresie faktycznego wykorzystania przez zawody prawnicze nowych technologii wskazują nadto, iż ta grupa zawodowa nie wykorzystuje maksymalnego poziomu potencjału oferowanego przez możliwości jakie dostarczają rozwiązania innowacyjne. Bezpośrednią przyczyną tego zjawiska jest przede wszystkim konieczność zapewnienia możliwie najwyższych standardów bezpieczeństwa, co nie zawsze jest możliwe do osiągnięcia w przypadku nowoczesnych rozwiązań. Co więcej, zdecydowana większość pracy tej grupy zawodowej oparta jest o rozwiązania legislacyjne, które kategorycznie regulują pewne możliwości. Niemniej jednak, wprowadzenie pewnych, chociażby niewielkich modyfikacji

przez prawodawcę pozwoliłoby na wprowadzenie rozwiązań i zabiegów, które pozwoliłyby na wykorzystanie potencjału sztucznej inteligencji w większym stopniu aniżeli aktualnie, a nadto zapewniłyby większą realizację celów jakie ma osiągać konkretna grupa zawodowa. Potencjał nowych technologii zdaje się być bardzo obiecujący, istotą jest możliwość skorzystania z jego możliwości, a w obliczu sukcesywnie wprowadzanych przez prawodawcę rozwiązań pozwala na pełne nadziei oczekiwanie na dalszą informatyzację wszystkich wspomnianych grup zawodowych, przy respektowaniu aktualnych możliwości i przepisów prawnych regulujących wspomiane kwestie, zarówno na poziomie krajowym, unijnym jak i europejskim.

Zważywszy na potęgę nowych technologii, doskonałym podsumowaniem czynionych na tle niniejszej pracy rozważań będzie cytat, zgodnie z którym „*The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life*" Billa Gates'a (postęp technologii polega na dostosowaniu jej tak, abyś nawet jej nie zauważał i tak by mogła stać się częścią codziennego życia).

WYKAZ LITERATURY WYKORZYSTANEJ W PRACY

1. Ahmed M., Shumailov I., Anderson R., *Tendrils of Crime: Visualizing the Diffusion of Stolen Bitcoins*, w: *Graphical Models for Security*, red. G. Cybenko, D. Pym, B. Fila, Springer International Publishing 2018.
2. Alelyani S., Kumar H., *Overview of Cyberattack on Saudi Organizations*, „Journal of Information Security and Cybercrimes Research" 2018/1.
3. Amato C., *Traditional Liability Requirements and New Sources of Damages* [w:] *Liability for Artificial Intelligence and the Internet of Things*, red. S. Lohsse, R. Schulze, D. Staudenmayer, Baden-Baden 2019.
4. Arkuszewska A.M., *Informatyzacja postępowania arbitrażowego,* Wolters Kluwer, 2019.
5. Banasiński C., *Cyberbezpieczeństwo*. Zarys wykładu, Wolters Kluwer, Warszawa 2018.
6. Banasiński C., Rojszczak M., *Cyberbezpieczeństwo,* Wolters Kluwer, Warszawa 2020.
7. Barcik J., *Niezawisłość sędziowska jako wartość konstytucyjna Unii Europejskiej. Glosa do wyroku Trybunału Sprawiedliwości z dnia 27 lutego 2018 roku, C 64/16,* 2018.
8. Bartosiewicz A. Kubacki R. PIT. Komentarz, wyd. V, Lex Wolters Kluwer Business, 2015.
9. Bartoszek M., *Zastosowanie sztucznej inteligencji w sądownictwie w świetle zasady skutecznej ochrony sądowej*, Folia Iuridica Univeristatis Wratislavieninsis.
10. Behan A., *Waluty wirtualne jako przedmiot przestępstwa,* Krakowski Instytut Prawa Karnego Fundacja, Kraków 2022.
11. Bhardwaj C., *Blockchain vs DLT – An Explanatory Guide You Can't Miss On.*
12. Białecki M. (red.), Kotas-Turoboyska S. (red.), Manikowski F. (red.), Słyk J. (red.), Szczepanowska E. (red.), *Rozstrzyganie spraw cywilnych. Aktualne wyzwania i perspektywy*, Wolters Kluwer, Warszawa 2022.
13. Biskup R., Ganczar M. *Komunikacja elektroniczna w postępowaniu administracyjnym,* Państwo i Prawo 2008/1/59-71.
14. Blicharz J. (red.), Zacharko L. (red.), *Administracja. Prawo administracyjne. Część ogólna*, Katowice 2018.
15. Blicharz J., *Administracja publiczna i społeczeństwo obywatelskie w państwie prawa,* Prawnicza i Ekonomiczna Biblioteka Cyfrowa, 2012.
16. Blicharz J., *W kwestii modelu współczesnej polskiej administracji publicznej,* Przegląd Prawa i Administracji, Tom 77, 2008.
17. Blicharz J., *Zakres znaczeniowy pojęcia „zadania publiczne"*, Przegląd Prawa i Administracji, t. LXXI, 2005.

18. Brenner S.W., *Cybercrime and the Law. Challenges. Issues, and Outcomes*, Boston 2012.
19. Brewster T., *All That's Needed to Hack Gmail and Rob Bitcoin: A Name and a Phone Number.*
20. Broadhurst R., Lord D., Maxim D., Woodford-Smith H., Johnston C., Woon Chung H.
21. Buat-Ménard É., „*Predictive" justice: Requirements, risks, and expectations – the experience in France*, „Les Cahiers de la Justice" 2019/2.
22. Bujalski R., *Akt o sztucznej inteligencji [Projekt UE] Komentarz praktyczny*, LEX, 2022
23. Bujalski R., *Odpowiedzialność za sztuczną inteligencję [Projekt UE] Komentarz praktyczny*, LEX, 2022.
24. Bytniewski A., *Wpływ systemów informatycznych na rozwój społeczeństwa informacyjnego*, Ekonomiczne Problemy Usług nr 105, 13-21, 2013.
25. Calo R., *Robots in American Law*, „Legal Studies Research Paper" 2016/4.
26. Caroll S., Trivedi H., Sabol B., *Malware Trends on 'Darknet' Crypto-Markets: Research Review*, Australian National University Cybercrime Observatory 2018.
27. Casey E., Daywalt C., *Computer Intrusions* (w:) E. Casey (red.), *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, Waltham–San Diego–London 2011.
28. Chałubińska-Jentkiewicz K., Karpiuk M. *Prawo nowych technologii. Wybrane zagadnienia,* Wolters Kluwer Polska, Warszawa 2015.
29. Chałubińska-Jentkiewicz K., *Prawna ochrona treści cyfrowych,* Wolters Kluwer, 2021.
30. Chałubińska-Jentkiewicz K., *Rozwój nowoczesnych technologii w kontekście procesu stanowienia prawa na przykładzie strategii AI*, Teka Komisji Prawniczej PAN Oddział w Lublinie, t. XII, 2019.
31. Chęć-Małyszek A., *Kultura społeczeństwa sieci a bezpośrednie kontakty społeczne,* Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy nr 31 (2)/2019.
32. Chmieliński P., *Środki komunikacji elektronicznej wykorzystywane w postępowaniu administracyjnych*, Przegląd Prawa Publicznego 2015/11/38-48.
33. Chmielnicki P. (red.), Mnich D. (red.), *Prawo jako projekt przyszłości*, Wolters Kluwer, Warszawa 2022.
34. Ciechomska M., *E-usługi a RODO*, Wolters Kluwer 2021.
35. Czaplicki K. (red.), Gryszczyńska A. (red.), Szpor G. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz,* Wolters Kluwer, 2019.

36. Dajnowicz-Piesiecka D. (red.), Jurgielewicz-Delegacz E. (red.), Pływaczewski E. W. (red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku*, 2022.
37. Dajnowiocz-Piesiecka D. (red.), Jurgielewicz-Delegacz E. (red.), Pływaczewski E. W. (red.), *Badania kryminologiczne a praktyka. Perspektywa krajowa i międzynarodowa,* 2021.
38. Dąbrowska J., *Charakter prawny bitcoin*, „Człowiek w Cyberprzestrzeni" 2017, nr 1.
39. Dmowska A., Podręczny słownik przysłów i powiedzeń, Delta W-Z, 2004.
40. *Do Web Hosts Protect Their Small Business Customers With Secure Hosting And Anti-Phishing Technologies? The Federal Trade Commission Staff Perspective*.
41. Domagała M., *Prawnokarna ochrona prywatności użytkowników Internetu,* Państwo i Prawo 2010/3/75-86.
42. Drajewicz D., *Kryteria powołania na stanowisko sędziego,* Przegląd Sądowy 2017/2/77-87.
43. Dudka K. (red.), *Kodeks postępowania karnego. Komentarz,* wyd. II, 2020.
44. Dudka K. (red.) *,Kodeks postępowania karnego. Komentarz*, Wolters Kluwer 2020.
45. Duniewska Z. (red.), Karcz-Kaczmarek M. (red.), Wilczyński P. (red.), *Prawo administracyjne w służbie jednostki i wspólnoty,* Wolters Kluwer, Warszawa, 2022.
46. Dymitruk M., Prawo sztucznej *inteligencji*, red. Świerczyński M, CH Beck, 2020.
47. Dziedzic K., *Jak skutecznie zapewnić sobie anonimowość. Anonimowość w Internecie. Kompletny poradnik krok po kroku, „Komputer i Świat"*, 2018 nr 1.
48. Fajgielski P. Automatyczne rozpoznawanie twarzy – wybrane zagadnienia prawne [w:] Fischer B. (red.), Pązik A. (red.), Świerczyński M. (red.), Prawo sztucznej inteligencji i nowych technologii, 2021.
49. Fajgielski P., *Informacja w administracji publicznej, prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007.
50. Filipkowski W. (red.), Pływaczewski E. (red.), Rau Z. (red.), *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne,* Wolters Kluwer, 2015.
51. Filipkowski W. *Prawo karne wobec sztucznej inteligencji, [w:] Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa: Wydawnictwo C.H. Beck 2020.
52. Filipkowski W., *Przestępczość z użyciem komputerów i ich sieci* [w:] Pływaczewski E. (red.) *Kryminologia. Stan i perspektywy rozwoju*, Wolters Kluwer, 2019.
53. Fischer B. (red.), Pązik A. (red.), Świerczyński M. (red.), *Prawo* sztucznej inteligencji *i nowych technologii*, Wolters Kluwer, Warszawa 2021.

54. Fischer B. (red.), Pązik A. (red.), Świerczyński M. (red.), *Prawo* sztucznej inteligencji *i nowych technologii*, Wolters Kluwer, Warszawa 2021.
55. Fischer B. (red.), Pązik A. (red.), Świerczyński M. (red.), *Prawo sztucznej inteligencji i nowych technologii 2*, Wolters Kluwer, Warszawa 2022.
56. Flaga-Gieruszyńska K., Gołaczyński J., *Prawo nowych technologii*, Wolters Kluwer, 2021.
57. Florczak-Wątor Monika [w:] Tuleja P. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wyd. II*, 2021.
58. Garlicki L. (red.), Zubik M. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom I, wyd. II*, Wyd. Sejmowe, 2016.
59. Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 1999 r. Wydawnictwo Fundacji Postępu Telekomunikacji.
60. Goc M., Gruza E., Moszczyński J., *Kryminalistyka czyli o współczesnych metodach dowodzenia przestępstw*, Wolters Kluwer, 2020.
61. Godlewska S., *Analiza kryminalna w postępowaniu karnym,* Prokuratura i Prawo 2022/3/55-72.
62. Godlewska-Michalak B. (red.), *Urząd sędziego koroną zawodów prawniczych. Materiały pokonferencyjne, Warszawa, 22 kwietnia 2008 r.*, Warszawa 2008.
63. Gomularz M., Świadczenie usług drogą elektroniczną. Komentarz. Wolters Kluwer, Warszawa 2019.
64. Gonet W. (red.), *Prawo o notariacie. Komentarz,* Wolters Kluwer, 2022.
65. Gorzkowska K., *Odpowiedzialność za działania sztucznej inteligencji* [w:] Kidyba Andrzej (red.), Olejniczak Adam (red.), *Nowoczesne technologie. Szansa czy zagrożenie dla funkcjonowania przedsiębiorców w obrocie prawnym i postępowaniach sądowych*, Wolters Kluwer, 2022.
66. Grajewski A. *Art. 11 – kwalifikacje niezbędne przy powołaniu* [w:] Simbierowicz M. (red.), Świtkowski M. (red.), *Komentarz do ustawy o komornikach sądowych. Ustawa o komornikach sądowych. Ustawa o kosztach komorniczych. Komentarz, wyd. III,* Wolters Kluwer, 2023.
67. Gryszczyńska A., Nowa Księga Wieczysta. Informatyzacja rejestru publicznego, Lexis Nexis 2011.
68. Gryszczyńska A., *Nowe zagrożenia bezpieczeństwa rejestrów publicznych*, [w:] Szpor G. (red.), Gryszczyńska A. (red.) *Internet. Strategie bezpieczeństwa*, Warszawa 2017.
69. Gryszczyńska A., *Tajemnica korespondencji*, Monitor Prawniczy 2015/24.

70. Grześkowiak M. *Udział obywateli w sprawowaniu wymiaru sprawiedliwości w państwach demokratycznych*, [w:] Piotrowski R. (red.) *Udział obywateli w sprawowaniu wymiaru sprawiedliwości*, 2021.
71. Grzybkowski M., Bentyn S., *Kryptowaluty. Dlaczego jeden bitcoin wart będzie milion dolarów?*, Poznań 2018.
72. Gurak K., Postęp techniczny i wynikająca z niego cyberprzestępczość jako wyzwanie współczesnej kryminologii [w:] Dajnowicz-Piesiecka D. (red.), Jurgielewicz-Delegacz E. (red.), Pływaczewski E.W.(red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku,* 2022.
73. Haczkowska M. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz.,* LexisNexis 2014.
74. Hildebrandt 2006, s. 548– 552; Bosco i in. 2015.
75. HLEG *AI* Definition 2018: The European Commission's High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main capabilities and scientific disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI*, Brussels 2018.
76. Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*. Poznań 2018, Wydawnictwo FNCE.
77. Hostettler O., *Darknet, Die Schattenwelt des Internets*, Zurych 2017.
78. Jacyszyn J., *„Wolny zawód" – anachronizm czy istotne pojęcie prawne?,* Przegląd Prawa Handlowego 2015/11/14-19.
79. Jacyszyn J., *Wykonywanie wolnych zawodów w Polsce,* Lexis Nexis 2004.
80. Jagielska M., *Odpowiedzialność za sztuczną inteligencję* [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa 2020.
81. Jankowska-Proch I., *Odpowiedzialność karna a działalność autonomicznych robotów. Wyzwania prawne i etyczne w polskim i światowym dyskursie naukowym* [w:] Chmielnicki Paweł (red.), Minich Dobrochna (red.), Prawo jako projekt przyszłości, 2022.
82. Janowski J, *Trendy cywilizacji informacyjnej. Nowy technototalitarny porządek świata*, Warszawa 2019.
83. Janowski J., *Elektroniczny obrót prawny*, Seria Akademicka Prawo, Warszawa 2008.
84. Jasińska K., *E-rozprawa w postępowaniu cywilnym a możliwość obrony swych praw w kontekście problemów z jej przeprowadzeniem* [w:] Fischer B. (red.), Pązik A. (red.), Świerczyński M. (red.), *Prawo sztucznej inteligencji i nowych technologii 2*, Wolters Kluwer, Warszawa 2022.

85. Jaworski Cz., *Urząd sędziego koroną zawodów prawniczych?* [w:] Hofmański P. (red.) *Fiat iustita pereat mundus. Księga jubileuszowa poświęcona Sędziemu Sądu Najwyższego Stanisławowi Zabłockiemu z okazji 40-lecia prawcy zawodowej*, Lexis Nexis 2014.
86. Jedlińska R., *Problem przestępczości elektronicznej*, „Elektroniczne Problemy Usług" 2017/1.
87. Kamińska K., *Zjawisko kradzieży tożsamości – aspekty prawne i kryminologiczne* [w:] Dajnowicz-Piesiecka Diana (red.), Jurgielewicz-Delegacz Emilia (red.), Pływaczewski Emil W. (red.), *Przestępczość XXI wieku. Szanse i wyzwania dla kryminologii*, 2020.
88. Kanty T., *Doświadczenie życiowe o ocena dowodów w procesie karnym,* Państwo i Prawo 2018/7/23-37.
89. Kasiński J. [w:] Świecki D. (red.), *Kodeks postępowania karnego. Orzecznictwo,* Wolters Kluwer, 2022.
90. Kaźmierczyk A. (red.), Michałowska K. (red.) Szaraniec M. (red.), *Verba volant, scripta mandet. Księga jubileuszowa dedykowana Pani Profesor Bogusławie Gneli,* 2023.
91. Kidyba A. (red.), Olejniczak A. (red.), *Nowoczesne technologie. Szansa czy zagrożenie dla funkcjonowania przedsiębiorców w obrocie prawnym i postępowaniach sądowych*, 2022.
92. Kiedrowicz-Wywoał A., *Pharming i jego penalizacja*, Prokuratura i Prawo 2011/6.
93. Kim C.H., Kriwoluzky A., *Public or Private? The Future of Money*, Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2019.
94. Kiziński M, *Retencja danych telekomunikacyjnych,* Prokuratura i Prawo 2016/1/138-155.
95. Koch R., *Legal Tech i nowoczesne technologie w pracy prawników wewnętrznych* [w:] Dzioba K. (red.), Rybicki R. (red.), *Metodyka pracy prawnika in-house*, 2021.
96. Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004.
97. Kosiński J., *Cyberprzestępczość* [w:] *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, 2013.
98. Kotecka S. [w:] *Informatyzacja postępowania sądowego w prawie polskim i wybranych państw*, pod red. J. Gołaczyńskiego, Biblioteka Sądowa.
99. Kotecka-Kral S., *Informatyzacja działalności korporacji prawniczych na przykładzie postępowania cywilnego* [w:] Flaga-Gieruszyńska K. (red.), Gołaczyński J. (red.), Prawo Nowych Technologii, Wolters Kluwer, 2021.
100. Krasuski A, Wolska-Bagińska A., Zienkiewicz-Będźmirowska O, Działania naruszające prawa do domen internetowych, Wolters Kluwer, 2021.

101. Krasuski A., *Prawa i obowiązki abonentów usług telekomunikacyjnych*, 2021.
102. Krasuski A., Prawa i obowiązki abonentów usług telekomunikacyjnych, Wolters Kluwer, Warszawa 2021.
103. Krasuski A., *Prawo telekomunikacyjne. Komentarz.*, wyd. IV, 2015.
104. Krysiński Ł., *Identyfikacja cyberprzestępców*, Prok. I Pr. 2020/2/120-134.
105. Księżak P., *Zawieranie umów przez sztuczną inteligencję* [w:] Dumkiewicz M. (red.), Kopaczyńska-Pieczniak K. (red.), Szczotka Jerzy (red.), *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie. Tom II*, 2020.
106. Kudła J., *Retencja danych a prawo UE*. Omówienie wyroków TS z dnia 20 września 2022 r., C-793/19 i C-794/19 (SpaceNet i in.) oraz C-339/20 i C-397/20 (VD i SR), 2022.
107. Kuliński M., *Regulacje Komunikacji Elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej*, CH Beck, Warszawa 2010.
108. Kurowski M. [w:] Świecki D. (red.), *Kodeks postępowania karnego. Tom I. Komentarz,* Wolters Kluwer, Warszawa, 2023.
109. Kusak M., Pawłowski T., *Zawody prawnicze a sztuczna inteligencja*, Rynek Pracy 2020.
110. Kusak M., Wiliński P., *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Wolters Kluwer, 2020.
111. Kwietko-Bębnowski M. *Informatyzacja sądów administracyjnych – próba oceny i poradnik praktyczny*, Przegląd Podatkowy 2020/6/42-48.
112. Lightbourne J., *Damned Lies & Criminal Sentencing using evidence-based tools*, 15 *D*uke *L*aw *&* *T*echnology *Review*, 2017.
113. Litwiński P., *Naruszenia bezpieczeństwa danych osobowych obejmujących numer PESEL – analiza ryzyka,* [w:] Matan A. (red.) *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza*, Wolters Kluwer, 2022.
114. Lubasz D., Namysłowska M., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną w: Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, Wolters Kluwer, Warszawa 2011.
115. Lugano G., Hudák M., Ivančo M., Loveček T., *From the Mind to the Cloud: Personal Data in the Age of the Internet of Things* [w:] *AI Love you*, red. Y. Zhou, M.H. Fischer, Cham 2019.
116. Łysik Ł., Kutera R., *Technologie mobilne jako determinanta rozwoju innowacyjnego społeczeństwa informacyjnego,* Ekonomiczne Problemy Usług nr 105, 33-44, 2013.

117. Machnacz A., *Gromadzenie i zabezpieczanie materiału dowodowego w zakresie przestępstw komputerowych* [w:] red. Kosiński J. *Przestępczość teleinformatyczna*, 2014.
118. Machnikowska A., *Zasada jawności w postępowaniu procesowym – modernizacja czy marginazliacja? Wybrane zagadnienia,* Polski Proces Cywilny 2022/1/80-124.
119. Mamak K. *Rewolucja cyfrowa a prawo karne*, Krakowski Instytut Prawa Karnego Fundacja, 2019.
120. Marcinkowska M., *Egzekucja komornicza z kryptowalut,* Przegląd Prawa Handlowego, 2021/6/12-16.
121. Martyniak G., Wojciechowski A., *Metodyka czynności w sprawach przestępstw popełnianych z wykorzystaniem sieci Internet*, (w:) Kosiński J., Kmiotek S.(red.), *Przestępczość Teleinformatyczna*, 2011.
122. Mielczarek-Mikołajów J., *Ochrona danych osobowych z perspektywy rozwoju e-administracji* [w:] Jędrzejczak M. (red.), *Ochrona danych osobowych w prawie publicznym,* Wolters Kluwer, 2021.
123. Monarcha-Matlak A., *Automated decision-making in public administration,* Procedia Computer Science 192 (2021): 2077-2084
124. Monarcha-Matlak A., *Komunikacja elektroniczna, prawo komunikacji elektronicznej, Europejski kodeks łączności elektronicznej i ich wpływ na rozwój jurysdykcji administracyjnej* [w:] Kruś M. (red.), Staniszewska L. (red.), Szewczyk M. (red.) *Kierunki rozwoju jurysdykcji administracyjnej*, Wolters Kluwer, Warszawa 2022.
125. Monarcha-Matlak A., *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Business, 2008.
126. Monarcha-Matlak A., *Pojęcie komunikacji elektronicznej w doktrynie i w aktach prawnych*, Lingwistyka Stosowana 24: 4/ 2017.
127. Monarcha-Matlak A., *Prawo administracyjne dziś i jutro*, red. Jagielski J., Wierzbowski M., Wolters Kluwer, 2018.
128. Monarcha-Matlak A., *Wzorce i zasady obecnej i przyszłej administracji publicznej* [w:] Jaworska-Dębska B. (red.), Kledzik P. (red.) Sługocki J. (red.) *Wzorce i zasady działania współczesnej administracji publicznej*, Wolters Kluwer, 2020.
129. Morison J., Harkens A., Re-engineerig justice? Robot judges, computerised courts and (semi) automated legal decision-making, Queen's University Belfast, "Legal Studies" 2019, t. 39, nr 4.
130. Mozgawa M. (red.), *Kodeks karny, komentarz aktualizowany*, LEX, 2023.

131. Nowina-Konopka M. *Istota i rozwój społeczeństwa informacyjnego* [w:] *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, red. M. Witkowska, K. Cholawo-Sosnowska, Warszawa 2006.
132. Oleszko A., *Prawo o notariacie. Komentarz. Tom 1. Ustrój notariatu,* Wolters Kluwer, 2016.
133. Opitek P., *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego,* Prokuratura i Prawo 2017/6/36-59.
134. Opitek P., *Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych,* Prokuratura i Prawo 2018/7-8/65-85.
135. Opracowania tematyczne, Kancelaria Senatu Biuro Analiz i Dokumentacji, listopad 2013.
136. Osmańska-Furmanek W., Furmanek M., *Technologie informacyjne cel czy narzędzie,* Chowanna 1, 132-149, 2006.
137. Pietrasz P. *Informatyzacja polskiego postępowania przed sądami administracyjnymi a jego zasady ogólne*, Wolters Kluwer, 2020.
138. Pietrasz P. *Konstytucyjne uwarunkwoania informatyzacji postępowania przez sądami administracyjnymi*, Zeszyty Naukowe Sądownictwa Administracyjnego 2016/2/38-48.
139. Polański P., *Usługi społeczeństwa informacyjnego na tle reformy usług Unii Europejskiej*, Quo Vafis Europo.
140. Potejko P., *Bezpieczeństwo informacyjne*, Warszawa, 2009.
141. Radoniewicz F., Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym kompiuterowym i systemom informatycznym, Wolters Kluwer, 2016.
142. Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, „Prawo w Działaniu" 2013/13.
143. Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
144. Rahman F., COMPAS Case Study: Fairness of a Machine Learning Model, "Towards Data Science", 7 września 2020.
145. Raport Głównego Urzędu Statystycznego, Społeczeństwo Informacyjne w Polsce w 2022.
146. Rejmaniak R., *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, Roczniki Nauk Prawnych Tom XXXI, numer 3-2021.
147. Rogalski M. (red.), Prawo *telekomunikacyjne. Komentarz*. LEX 2010.

148. Rogalski M., *Udostępnianie danych telekomunikacyjnych sądom i prokuratorom*, Prokuratura i Prawo 2015, nr 12.

149. Rojszczak M., *Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna,* Państwo i Prawo 2023/2/33-58.

150. Różanowski K., *Sztuczna inteligencja: Rozwój, szanse, zagrożenia*, Zeszyty Naukowe 109-135, 2007..

151. Russell R. (red.), *Hack Proofing Your Network. Edycja Polska*, Gliwice 2002.

152. Rutkowski K., *Predictive justice – sprawiedliwość algorytmów* [w:] Dajnowicz-Piesiecka D. (red.), Jurgielewicz-Delegacz E. (red.), Pływaczewski E.W.(red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku,* 2022.

153. Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016, Warszawa 2010.

154. Sarnecki P., *Pojęcie zawodu zaufania publicznego (art. 17 ust. 1 Konstytucji na przykładzie adwokatury)* [w:] *Konstytucja. Wybory. Parlament. Studia ofiarowane Zdzisławowi Jaroszowi*, red. L. Garlicki, 2000.

155. Seweryn R., *Technologie informacyjne i komunikacyjne*, C.H. Beck, Warszawa 2017.

156. Skoczylas D., *Dynamizm legislacji administracyjnej a cyberbezpieczeństwo i użytkowanie przestrzeni kosmicznej w ramach e-administracji* [w:] Kruś M. (red.), Staniszewska L. (red.), Szewczyk M. (red.) *Kierunki rozwoju jurysdykcji administracyjnej,* Wolters Kluwer, Warszawa 2022.

157. Skolimowski M., *Polityka cyberbezpieczeństwa w świetle zagrożenia cyberterroryzmem*, [w:] Szpor G. (red.), Gryszczyńska A. (red.*) Internet. Strategie bezpieczeństwa*, Warszawa 2017

158. Skóra A., *Art. 47 Obowiązki operatora wyznaczonego w zakresie realizacji publicznej usługi hybrydowej; moc dowodowa wydruku dokumentu elektronicznego w ramach publicznej usługi hybrydowej* [w:] Kwiatek B. (red.), Skóra A. (red.) Doręczenia elektroniczne. Komentarz, Wolters Kluwer, 2023.

159. Sobczak J., *Niezawisłość sędziowska i niezależność sądów. Problem ważny i ciągle aktualny*, Gdańskie Studia Prawnicze Przegląd Orzecznictwa 2015/4/79-115.

160. Sołtyszewski I., Solodov D. *Procedury policyjne poszukiwań osób zaginionych* [w:] Gruza E. (red.), Sołtyszewski I. (red.), *Poszukiwania osób zaginionych,* Wolters Kluwer, 2021.

161. Stańczuk I., Dane osobowe jako „waluta" związana z uczestnictwem w mediach społecznościowych [w:] Chałubińska-Jentkiewicz K. (red.), Nowikowska M. (red.),

Wąsowski K. (red.), *Media w erze cyfrowej. Wyzwania i zagrożenia,* Wolters Kluwer, Warszawa 2021.

162. Staszczyk P., *Czy unijna regulacja odpowiedzialności za sztuczną inteligencję jest potrzebna*?, Europejski Przegląd Sądowy, 2022.

163. Stefański R. (red.), Zabłocki S. (red.), *Kodeks Postępowania Karnego. Tom III. Komentarz do art. 297-424.*

164. Stępień-Załucka B, *Sprawowanie wymiaru sprawiedliwości przez Sąd Najwyższy w Polsce*, Warszawa 2016.

165. Stryczyńska Ewa, Urząd sędziego koroną zawodów prawniczych.

166. Szostek D. *Czynność prawna a środki komunikacji elektronicznej*, Kraków 2004.

167. Szpor G. (red.), *Jawność i jej ograniczenia*, t. 1, *Idee i pojęcia*, Warszawa 2016.

168. Szpor G. [w:] *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz,* Wolter Kluwer Business, 2020.

169. Szpor G., *Administracyjnoprawne problemy informatyzacji*, [w:] Supernata J. (red.), *Między tradycją a przyszłością w nauce prawa administracyjnego. Księga jubileuszowa dedykowana Profesorowi Janowi Bociowi*, Wrocław 2009.

170. Szpor G., *Art. 3 Objaśnienia określeń użytych w ustawie* [w:] Martysz Cz. (red.), Szpor G. (red.), Wojsyk K. (red.), *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz,* Wolters Kluwer, 2015.

171. Szpor G., Gryszczyńska A., *Internet. Strategie bezpieczeństwa*, Warszawa 2017.

172. Szpor G., *Urzędnicy w społeczeństwie informacyjnym*, [w:] Niewiadomski Z. (red.), *Prawo administracyjne*, Warszawa 2007.

173. Szpor G., *Lex informatica – problemy słownika* [w:] *Informatyzacja postępowania sądowego i administracji publicznej*, red. J. Gołaczyński, Warszawa 2010.

174. Szymczak M., *Słownik języka polskiego*, t. 1–3, Państwowe Wydawnictwo Naukowe, Warszawa 1978–1981.

175. Ślęzak P., Prawo mediów, Wolters Kluwer, Warszawa 2020.

176. Tabernacka M., *Pojęcie zawodu zaufania publicznego*, AUWr. Przegląd Prawa i Administracji 2004/2663.

177. Taberski D. *Postępowania w sprawach o oszustwa popełnione za pośrednictwem Internetu,* Prokuratura i Prawo 2018/6/63-83.

178. Thiebes S., Lins S., Sunyaev A., Trustworthy artificial intelligence, "Electronic Markets" 2021, t. 31, nr 2.

179. Tkacz S., Tobor Z., *Prawo a nowe technologie, Wydawnictwo Uniwersytetu Śląskiego*, Katowice 2019.
180. Tuleja P. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Wyd. II*, 2021.
181. Turek P., *Prawo o prokuraturze. Komentarz.*, Wolters Kluwer, 2023.
182. Uliasz M., *Zasada jawności sądowego postępowania egzekucyjnego w dobie informatyzacji*, Wolters Kluwer, Warszawa, 2019.
183. Wagner B., *Nieskazitelność charakteru sędziego,* Przegląd Sądowy 2019/11-1/7-18.
184. Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego, 2013.
185. Wilbrandt-Gotowicz M. (red.), *Doręczenia elektroniczne. Komentarz*, Wolters Kluwer, 2021.
186. Witkowska M., Cholawo-Sosnowska K., *Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006.
187. Wojtczak K., Co to jest wolny zawód, Zeszyty Naukowe WSZiB, 1997.
188. Wojtczak K., *Co to jest wolny zawód*, Zeszyty Naukowe WSZiB 1997.
189. Wojtczak K., *Zawody zaufania publicznego, zawody regulowane oraz wolne zawody. Geneza, funkcjonowanie i aktualne problemy*, Kancelaria Senatu, Biuro Analiz i Dokumentacji.
190. Wolska-Bagińska A., *Metodyka prowadzenia postępowań w sprawach z wykorzystaniem domen internetowych* [w:] Krasuski A, Wolska-Bagińska A., Zienkiewicz-Będźmirowska O, *Działania naruszające prawa do domen internetowych*, Wolters Kluwer, 2021.
191. Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Uniwersytet w Białymstoku, Białystok 2017.
192. Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Wolters Kluwer, 2020.
193. Zalewski T., *Prawo Sztucznej Inteligencji*, C.H. Beck, Warszawa 2020.
194. Zamojski Ł., *Krajowy Rejestr Sądowy. Komentarz, wyd. II,* Wolters Kluwer, 2023.
195. Zielińska C. *„Cybercrime" – wzywanie dla kryminologii* [w:] Dajnowicz-Piesiecka Diana (red.), Jurgielewicz-Delegacz Emilia (red.), Pływaczewski Emil W. (red.), *Prawo karne i kryminologia wobec kryzysów XXI wieku*, 2022.
196. Zimna M., *Wyłączenie jawności rozprawy jako gwarancja ochrony interesów uczestników postępowania karnego*, Prokuratura i Prawo 2016/9/87-108.

197. Ziółkowska K., *Transformacja administracji w* e-administrację [w:] Wierzbowski M. (red.) *Postępowanie administracyjne i sądowoadministracyjne*, Warszawa 2020.

WYKAZ AKTÓW PRAWA KRAJOWEGO

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.).
2. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2023 r. poz. 775).
3. Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2021 r. poz. 1805 ze zm.).
4. Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2022 r. poz. 1184, 1268).
5. Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (Dz.U. z 2022 r. poz. 1166).
6. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2023 r. poz. 171).
7. Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie (Dz.U. z 2022 r. poz. 1799).
8. Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. z 2023 r. poz. 28 ze zm.).
9. Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz.U. z 2023 r. poz. 1234).
10. Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (Dz. U. z 2022 r. poz. 2587 ze zm.).
11. Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2023 r. poz. 120, 295).
12. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz.U. z 2022 r. poz. 1138 ze zm.).
13. Ustawa z dnia 6 czerwca 1997 r. Kodeks Postępowania Karnego (Dz.U. z 2022 r. poz. 1275 ze zm.).
14. Ustawa z dnia 21 sierpnia 1997 r. o ochronie zwierząt (Dz. U. z 2022 r. poz. 572, 2375).
15. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. ze zm.).
16. Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2023 r. poz. 1068).
17. Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce (M.P. 2000 nr 22 poz. 448).
18. Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz. U. z 2022 r. poz. 2556 ze zm.).
19. Ustawa z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych (Dz. U. z 2022 r. poz. 2448).

20. Ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2023 r. poz. 217).
21. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902).
22. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344).
23. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648 ze zm.).
24. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57, 1123, 1234).
25. Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz.U. z 2023 r. poz. 172).
26. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. 2007 nr 10 poz. 68).
27. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r. poz. 122).
28. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2023 r. poz. 756, 1030).
29. Ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze (Dz. U. z 2023 r. poz. 1360).
30. Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz. U. 2016 poz. 508).
31. Ustawa z dnia z 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2021 r. poz. 2234 ze zm.).
32. Ustawa z dnia 28 lutego 2018 r. o kosztach komorniczych (Dz. U. z 2023 r. poz. 1357).
33. Ustawa z dnia 22 marca 2018 r. o komornikach sądowych (Dz. U. z 2023 r. poz. 590, 614).
34. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913).
35. Zarządzenie nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji (Dz. Urz. KGP 2019 poz. 114).
36. Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2023 r. poz. 1327).
37. Zarządzenie nr 28 Komendanta Głównego Policji z dnia 11 sierpnia 2020 r. w sprawie zbiorów danych daktyloskopijnych (Dz. Urz. KGP 2020 poz. 44).

38. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. z 2023 r. poz. 285).
39. Uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 roku w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020", Monitor Polski 2021 poz. 23.
40. Ustawa z dnia 9 czerwca 2022 roku o wspieraniu i resocjalizacji nieletnich (Dz. U. 2022 poz. 1700).
41. Rozporządzenie Ministra Finansów z dnia 28 lutego 2023 r. w sprawie przechowywania w Centralnym Repozytorium Elektronicznych Wypisów Aktów Notarialnych aktów notarialnych, zarejestrowanych aktów poświadczenia dziedziczenia i zarejestrowanych europejskich poświadczeń spadkowych (Dz. U. 2023 poz. 378).

WYKAZ AKTÓW PRAWA MIĘDZYNARODOWEGO I UNIJNEGO

1. Konwencja Rady Europy nr 108 z dnia 24 października 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. z 2003 r. Nr 3, poz. 25).
2. Dyrektywa 98/48/WE Parlamentu Europejskiego i Rady z dnia 20 lipca 1998 r. zmieniająca dyrektywę 98/34/WE ustanawiającą procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz. Urz. UE.L.1998.217.18).
3. Dyrektywa 000/31 Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz. U. UE L 2000.178.1).
4. Konwencja Rady Europy z dnia 23 listopada 2001 r. o cyberprzestępczości (Dz. U. 2015 poz. 728).
5. Dyrektywa 2002/21/WE z dnia 7 marca 2002 r. o wspólnych ramach regulacyjnych dla sieci usług komunikacji elektronicznej (Dz. U. UE. L.2002.108.51).
6. Dyrektywa Komisji 2002/77/WE z dnia 16 września 2002 r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej (Dz. U. UE. L.2002.249.21).
7. Dyrektywa UE 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. U. UE L 241/1).
8. Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w s

sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE 4.5.2016).
9. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (Dz. U. L 194 z 19.7.2016).
10. Dyrektywa Parlamentu Europejskiego i Rady UE 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz. U. UE L 321/36).
11. Rezolucja Parlamentu Europejskiego zawierającej zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL).
12. Komunikat Komisji Europejskiej z dnia 25 kwietnia 2018 r., Sztuczna Inteligencja dla Europy, COM (2018) 237 final.
13. Biała Księga w sprawie sztucznej inteligencji. Europejskie Podejście do doskonałości i zaufania. Komisja Europejska, 19 lutego 2020 r. COM (2020) 65 final.
14. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii Europejskiej z dnia 21 kwietnia 2021 r.
15. Rezolucja Parlamentu Europejskiego z dnia 3 maja 2022 r. w sprawie sztucznej inteligencji w epoce cyfrowej (Dz. U. UE. C.2022.465.65).

WYKAZ ORZECZEŃ

1. Wyrok Trybunału Sprawiedliwości z dnia 11 września 2014 r. sygn. C-291/13, EU:C:2014:2209, pkt 28, 29.
2. Wyrok Sądu Najwyższego Stanu Wisconsin z 13 lipca 2016 r. w sprawie State przeciwko Loomis, sygn. 881 N.W.2d 749 (2016).
3. Wyrok Naczelnego Sądu Administracyjnego z dnia 18 maja 2017 r. sygn.. II FSK 454/17.
4. Wyrok Sądu Apelacyjnego w Białymstoku z dnia 16 listopada 2017 r., sygn. II AKa 178/17, LEX nr 2437805.
5. Wyrok Sądu Apelacyjnego w Warszawie z dnia 20 grudnia 2018 r. sygn. II AKa 420/18, LEX nr 2622689.
6. Wyrok Sądu Apelacyjnego w Warszawie z dnia 23 października 2019 roku sygn. II AKa 382/18, LEX nr 2759496.
7. Wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 24 czerwca 2020 roku sygn.. III SA/GI 138/20, LEX nr 3040660.

8. Postanowienie Sądu Najwyższego z dnia 3 listopada 2021 roku, sygn. III KK 320/21, LEX nr 3275322.
9. Wyrok Sądu Najwyższego z dnia 23 marca 2022 r. sygn. I NKRS 18/22.
10. Wyrok Sądu Okręgowego w Siedlcach z dnia 18 maja 2022 roku, sygn.. II Ka 198/22, LEX nr 3353329.
11. Por. Wyrok Sądu Rejonowego w Chełmnie z dnia 18 kwietnia 2023 r. sygn. I C 433/21, LEX nr 3574487.

Inne źródła

1. Bell J., Schneier B., Greenwald G., *NSA and GCHQ target Tor network that protects anonymity of web users*, www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (dostęp: 10.06.2023 r.)
2. Haas P., *The real reason to be afraid of Artificial Intelligence*, konferencja TEDx, Dirigo, listopad 2017, https://www.ted.com/talks/peter_haas_the_real_reason_to_be_afraid_of_artificial_intelligence (dostęp: 01.04.2023 r.)
3. http://ec.europa.eu/ information_society/tl/help/glossary/index_en.htm#c (dostęp: 5.02.2023 r.)
4. http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2013/p111.pdf (dostęp 10.05.2023 r.)
5. *https://appinventiv.com/blog/blockchain-vs-dlt-guide/* (dostęp: 20.06.2023 r.)
6. https://blogs.lse.ac.uk/businessreview/2021/08/16/artificial-intelligence-liability-the-rules-are-changing/ (dostęp: 07.02.2023 r.)
7. https://cli.re/LqnQ7d (dostęp: 01.06.2023 r.)
8. https://csirt.gov.pl/cer/publikacje/polityka-ochrony-cyber (dostęp: 5.02.2023 r.)
9. https://datareportal.com/reports/digital-2022-poland (dostęp: 01.06.2023 r.)
10. https://datareportal.com/reports/digital-2022-poland (dostęp: 2.03.2023 r.)
11. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0496&qid=1665410785599 (dostęp: 12.02.2023 r.)
12. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206&from=PL (dostęp: 12.02.2023 r.)

13. https://legaltechnology.com/2017/10/30/machine-beats-man-in-casecrunch-lawyer-challenge/ (dostęp: 15.06.2023 r.)
14. https://obtk.pl/slownik/chat-gpt-co-to-jest/ (dostęp: 30.05.2023 r.)
15. https://sjp.pwn.pl (dostęp 10.11.2022 r.)
16. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,2,12.html (dostęp: 30.06.2023 r.)
17. https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63976,Oszustwo-art-286.html (dostęp: 05.05.2023 r.)
18. https://uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2021-r-,431.html (dostęp 10.05.2023 r.)
19. https://www.coinbase.com/pl/price/bitcoin (dostęp: 10.07.2023 r.)
20. https://www.econstor.eu/bitstream/10419/55888/1/687133424.pdf (dostęp 2.03.2023 r.)
21. https://www.europarl.europa.eu/cmsdata/207653/13.%20PE%20642.356%20DIW%20final%20publication-original.pdf (dostęp: 15.06.2023 r.)
22. https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/?sh=5e10f64741a4 (dostęp: 10.07.2023 r.)
23. https://www.hootsuite.com (dostep: 2.03.2023 r.)
24. https://www.istshare.eu/ict-technologie-informacyjno-komunikacyjne.html (dostęp: 10.03.2023 r.)
25. https://www.oxfordinsights.com/government-ai-readiness-index-2022 (dostęp: 06.02.2022 r.)
26. https://www.pnas.org/doi/10.1073/pnas.2120481119 (dostęp: 02.06.2023 r.)
27. https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?id=66C7F7C637867159C12589170035C136 (dostęp: 31.03.2023 r.)
28. https://www.uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2020-r-,391.html (dostęp 10.05.2023 r.)
29. https://www-arch.polsl.pl/wydzialy/ROZ/ZN/Documents/zeszyt%20123/Stylec-Szromek.pdf (dostęp: 10.03.2023 r.)
30. Międzynarodowy projekt badawczy: *Cyberbezpieczeństwo Grupy Wyszehradzkiej na rzecz zapobiegania przyczynom przestępczości*, zrealizowany przez Instytut Wymiaru Sprawiedliwości https://iws.gov.pl/centrum- analiz-strategicznych/cyberbezpieczenstwo-grupy-wyszehradzkiej-na-rzecz-zapobiegania-przyczynom-przestepczosci/wiecej/ (dostęp 20.05.2023 r.)

31. stat.gov.pl (dostęp 28.02.2020 r.)
32. Żyłowska K., Czym jest uczenie maszynowe (Machine Learning)?, https://aibusiness.pl/czym-jest-uczenie-maszynowe-machine-learning/ (dostęp: 20.05.2023 r.)

Streszczenie rozprawy doktorskiej

pt. „Wpływ nowych technologii na funkcjonowanie zawodów prawniczych”

Nowe technologie odnoszą bezpośredni wpływ na wszystkie sfery życia, w tym społecznego i ekonomicznego. Nieustanny rozwój technologiczny kształtuje nie tylko sytuacje w życiu codziennym, ale także określa sytuacje prawne, powodując znaczący wpływ również na działalność wszystkich zawodów prawniczych. Określenie stopnia wpływu nowych technologii na funkcjonowanie tej grupy zawodowej stanowi ciekawy i istotny problem badawczy, który został poddany szczegółowemu badaniu w przedmiotowej rozprawie, w której przeanalizowano rzeczywisty wpływ postępu technologicznego na funkcjonowanie każdej z profesji prawniczych. W związku z tym przedstawiono zarówno faktyczne jak i hipotetyczne możliwości wykorzystania potencjału nowych technologii w odniesieniu do różnych grup zawodowych, oceniając jednocześnie przydatność omawianych rozwiązań oraz ich wpływ na funkcjonowanie i byt danej profesji. Badania w tym zakresie przeprowadzone zostały w odniesieniu do każdej z grup oddzielnie, tj. zawodów adwokata i radcy prawnego, notariusza, komornika, ale również wymiaru sprawiedliwości oraz organów ścigania, która to grupa dominowała wśród podejmowanych badań. Przed poczynieniem rozważań w tym zakresie, dokonano kompleksowej analizy istotnych pojęć występujących w ramach szeroko rozumianych nowych technologii, jak również omówiono teoretycznoprawne aspekty funkcjonowania zawodów prawniczych.

Wskutek poczynionych badań dotyczących faktycznego wpływu nowych technologii na funkcjonowanie zawodów prawniczych, możliwe było wytypowanie zarówno pozytywnych aspektów postępu technologicznego, jak również negatywnych jego następstw. Wśród takich jako najistotniejsze wyodrębniono zjawisko cyberprzestępczości, które z uwagi na rozwój społeczeństwa informacyjnego oraz nieustanny rozwój technologiczny, stało się dominującym wyzwaniem dla organów ścigania. Konieczność zapewnienia cyberbezpieczeństwa stanowi aktualnie naczelny problem dla tej grupy zawodowej. Udostępnienie coraz to bardziej innowacyjnych narzędzi, w powiązaniu z ogólnodostępnymi środkami zapewniającymi poczucie pozornej anonimowości dla sprawców cyberprzestępstw, sprawia, iż środowisko dla sprawców tego rodzaju czynów zabronionych staje się wręcz doskonałe. Zjawisko to wzmacnia dodatkowo fakt, iż większość usług w obecnie otaczającej rzeczywistości dostępna jest za pośrednictwem sieci teleinformatycznej, która jest przestrzenią dla cybersprawców. Możliwość zawarcia umów pożyczkowych i umów o otwarcie rachunku bankowego za pośrednictwem

Internetu, dokonywanie zakupów przez Internet na potężną skalę, komunikowanie się w przeważającej części za pośrednictwem komunikatorów społecznościowych, a także ogólne wykorzystanie aplikacji mobilnych sprawia, iż przestępstwa popełniane za pośrednictwem sieci teleinformatycznej stanowią dominującą liczbę przestępstw popełnianych na terenie kraju. Fakt ten z kolei oznacza znaczący i bezpośredni wpływ na pracę organów ścigania, które muszą dostosować algorytmy działania w procesie wykrywczym do rodzaju przestępstwa z jakim mają wówczas do czynienia. Inaczej przebiega proces wykrywczy w przypadku tzw. przestępstw powszechnych, a odmiennie w odniesieniu do cyberprzestępstw, w przypadku których ślady zostawiane są co do zasady wyłącznie w świecie wirtualnym i tam organy ścigania winny przenieść swoją metodykę działania. W rozprawie wyczerpująco omówiono przebieg procesu wykrywczego, sposoby przyjęcia właściwego modelu i algorytmu działania pod kątem zapewnienia maksymalizacji celów postępowania karnego, tj. wykrycia sprawcy i pociągnięcia go do odpowiedzialności karnej.

W związku z bezapelacyjnie występującym zjawiskiem cyberprzestępczości pozostającym w nierozerwalnym związku z postępem technologicznym oraz zaawansowanym poziomem społeczeństwa informacyjnego, w rozprawie poddano analizie status społeczeństwa informacyjnego w Polsce. W tym celu przeprowadzono badania ilościowe w odniesieniu do dwóch grup badawczych, o zróżnicowanych cechach, zarówno w aspekcie wieku, zatrudnienia oraz wykształcenia, co pozwoliło na uzyskanie rzetelnych i kompleksowych wyników w tym zakresie. Wskazane badania w sposób jednoznaczny potwierdziły tezę, iż społeczeństwo informacyjne w Polsce funkcjonuje na bardzo zaawansowanym poziomie, a wykorzystanie środków komunikacji elektronicznej jest dominującym sposobem porozumiewania się.

Sztuczna inteligencja bez wątpienia stanowi element rozwoju technologicznego, która z uwagi na swój charakter oraz potencjał, uznawana jest za zagrożenie dla bytu zawodów prawniczych. Z uwagi na coraz bardziej popularyzowane stanowisko, zgodnie z którym mechanizmy oparte o działanie sztucznej inteligencji mogą zastąpić zawody prawnicze, uznano, iż kwestia ta stanowi doniosły problem badawczy, który także stanowił punkt rozważań w rozprawie. W tym celu przeanalizowano narzędzia oparte głównie o uczenie maszynowe, które z powodzeniem funkcjonują w innych państwach w obrębie działalności zawodów prawniczych. Ocenie poddano również aktualne wykorzystanie potencjału sztucznej inteligencji w Polsce, zarówno w odniesieniu do branży prawniczej, jak również w życiu codziennym. Podjęto próbę oceny ryzyka faktycznej możliwości zastąpienia tej grupy zawodowej, które przy uwzględnieniu charakteru zawodów prawniczych, współpracy opartej o

stosunek zaufania, konieczności logicznego myślenia w powiązaniu z zasadami doświadczenia życiowego, nieustannymi zmianami legislacyjnymi, zostało ocenione jako niskie. W związku z tym przyjęto, iż w najbliższej przyszłości sztuczna inteligencja nie wpłynie na byt zawodów prawniczych, a może poprawić jakość funkcjonowania tej grupy zawodowej przy odpowiednim otwarciu się na jej potencjał.

Przeprowadzone badania dotyczące wykorzystania przez zawody prawnicze narzędzi opartych o działanie nowych technologii, pozwoliły nadto na wytypowanie postulatów, których wprowadzenie w przyszłości mogłyby wpłynąć na jakość realizowanych działań, usprawnić pracę zawodów prawniczych, zminimalizować czynnik czasu przy jednoczesnym poszanowaniu powszechnie obowiązujących zasad dotyczących poszczególnej grupy zawodowej. W związku z tym wskazano na narzędzia, które przy obecnych możliwościach prawodawcy, mogłyby zostać z powodzeniem wprowadzone. W tym aspekcie przeanalizowano również nadążanie prawodawcy nad nieustanną zmianą rzeczywistości rozpatrywanej w kontekście zmian technologicznych i odpowiednie reagowanie poprzez dokonywanie zmian regulacji prawnych w tym obszarze.

Kompleksowe i wszechstronne wyniki badań przeprowadzone w rozprawie potwierdziły postawioną na wstępie tezę, iż nowe technologie wywierają bezpośredni wpływ na funkcjonowanie zawodów prawniczych. Nie pozostawia wątpliwości fakt, iż rozwój technologiczny stał się nieprawdopodobną szansą aktualnej rzeczywistości i w przeważającej części zjawisko to należy ocenić pozytywnie. Niemniej jednak przytoczone fakty i okoliczności wprost dowodzą, iż nowe technologie stanowią także potężne zagrożenie, rozpatrywane zwłaszcza w zakresie cyberbezpieczeństwa. Zważywszy na potęgę nowych technologii, z nadzieją należy oczekiwać na wprowadzenie przez ustawodawcę nowych rozwiązań prawnych, pozwalających na maksymalne wykorzystanie ich potencjału.

W pracy uwzględniono stan prawny obowiązujący w dniu 30 czerwca 2023 r.

Summary of the doctoral dissertation

Entitled „The impact of new technologies on the functioning of legal professions"

New technologies have a direct impact on all spheres of life, including social and economic. Constant technological development shapes not only situations in everyday life, but also determines legal situations, causing a significant impact also on the activities of all legal professions. Determining the degree of impact of new technologies on the functioning of this professional group is an interesting and important research problem that has been subjected to a detailed study in the dissertation in question, in which the actual impact of technological progress on the functioning of each of the legal professions was analyzed. Therefore, both actual and hypothetical possibilities of using the potential of new technologies in relation to various professional groups were presented, while assessing the usefulness of the discussed solutions and their impact on the functioning and existence of a given profession. Research in this area was carried out for each of the separate groups, i.e. advocate and legal adviser, notary public, bailiff, but also the judiciary and law enforcement agencies, which group dominated among the research evidence. Before making considerations in this regard, an additional analysis of the concepts on broadly understood new technologies was made, as well as the theoretical and legal aspects of the functioning of legal professions were discussed.

As a result of the research on the actual impact of new technologies on the functioning of legal professions, it was possible to identify both the positive aspects of technological progress and its negative consequences. Among them, the phenomenon of cybercrime was singled out as the most important, which, due to the development of the information society and constant technological development, has become a dominant challenge for law enforcement authorities. The need to ensure cyber security is currently the main problem for this professional group. The availability of more and more innovative tools, combined with publicly available means that ensure a sense of apparent anonymity for cybercrime perpetrators, makes the environment for perpetrators of this type of prohibited act almost perfect. This phenomenon is additionally strengthened by the fact that most services in the current reality are available via the ICT network, which is a space for cyber perpetrators. Allowing the conclusion of a loan agreement and a bank account agreement via the Internet, making transactions via the Internet, communicating via social messengers, as well as the general use of a mobile applications, makes crime make through the ICT network is the most popular in the country. This fact, in turn, means the operation and impact on the operation of law enforcement agencies, which

require the combination of algorithms of action in the detection process to the type of action for the reason that they come to fruition. The detection process is different in the case of the so-called common crimes, and differently in relation to cybercrime, in the case of which traces are generally left only in the virtual world, and law enforcement authorities should transfer their methods of operation there. The dissertation comprehensively discusses the course of the detection process, the ways of adopting the appropriate model and algorithm of action in terms of ensuring the maximization of the goals of criminal proceedings, i.e. detecting the perpetrator and bringing him to justice.

Due to the indisputable phenomenon of cybercrime, which is inseparable from technological progress and the advanced level of the information society, the dissertation analyzes the status of the information society in Poland. For this purpose, quantitative research was carried out in relation to two research groups with different characteristics, both in terms of age, employment and education, which allowed to obtain reliable and comprehensive results in this regar. The indicated research clearly confirmed the thesis that the information society in Poland functions at a very advanced level, and the use of electronic means of communication is the dominant means of communication.

Artificial intelligence is an element of technological development, which, due to its nature and potential, is considered to be danger for the existence of legal professions. Due to the increasingly popular position that arificial intelligence could replace the lawyers, it was recognized that this is an important research problem, which is also a point of consideration in the dissertation. For this purpose, tools based mainly on machine learning, which successfully operate in other countries within the legal professions, were analyzed. The current use of the potential of artificial intelligence in Poland was also assessed, both in relation to the legal industry and in everyday life. An attempt was made to assess the risk of the actual possibility of replacing this professional group, which, taking into account the nature of legal professions, cooperation based on trust, the need for logical thinking in connection with the principles of life experience, constant legislative changes, was assessed as low. Therefore, it was assumed that in the near future artificial intelligence will not affect the existence of the legal professions, and it may improve the quality of functioning of this professional group with proper opening to its potential.

The conducted research on the use of tools based on new technologies by the legal professions also allowed for the selection of postulates, the introduction of which in the future could affect the quality of the activities carried out, improve the work of legal professions,

minimize the time factor while respecting the generally applicable rules for a particular professional group. Therefore, tools were indicated that could be successfully introduced with the current possibilities of the legislator. In this aspect, the legislator's keeping up with the constant change of reality considered in the context of technological changes and the appropriate response by amending legal regulations in this area were also analyzed.

Comprehensive research results carried out in the dissertation confirmed the thesis put forward at the beginning that new technologies have a direct impact on the functioning of legal professions. There is no doubt that technological development has become an incredible opportunity for the current reality, and for the most part of this phenomenon should be positively assessed. Nevertheless, the cited facts and circumstances directly prove that new technologies are also a powerful threat, especially in the field of cyber security. Given the power of new technologies, it is hoped that the legislator will introduce new legal solutions that will allow for the maximum use of their potential.

Legals status valid for June 30, 2023 is applicable to this study.

Załączniki

Załącznik nr 1 - Wzór kwestionariusza ankiety udostępnionej w pierwszej grupie badawczej

1. **Płeć:**
   a) Kobieta
   b) Mężczyzna
   c) Nie chcę wskazywać.
2. **Wiek:**
   a) 18-25 lat
   b) 26-40 lat
   c) 41-55 lat
   d) 56-68 lat
3. **Wykształcenie:**
   a) podstawowe
   b) zawodowe
   c) średnie
   d) wyższe
4. **Jak często korzystasz z Internetu w ciągu dnia?**
   a) Wcale
   b) Bardzo rzadko, tj. mniej niż 1 godzinę
   c) 2-4 godziny
   d) Powyżej 4 godzin
5. **W jakim celu przeważnie korzystasz z Internetu?** (możliwość zaznaczenia kilku odpowiedzi)
   a) Portale społecznościowe, Facebook itp.
   b) Informacje ze świata i kraju
   c) Poczta elektroniczna
   d) Opłata rachunków, załatwienie spraw
   e) Telewizja internetowa
   f) Rozrywka
   g) Nauka
6. **Za pomocą jakiego łącza korzystasz z Internetu?**
   a) Stałe łącze, sieć wifi domowa
   b) Otwarte/darmowe łącze w galeriach handlowych, pociągach, miejscach publicznych
   c) Transmisja danych od operatora sieci komórkowej w telefonie
7. **Skąd głównie czerpiesz informacje na temat sytuacji w kraju i na świecie?**
   a) Z telewizji
   b) Z Internetu

c) Od znajomych i współpracowników

d) Nie interesuje się tym

8. **Czy korzystasz z platform sprzedażowych typu Olx, Otomoto, Vinted, Marketplace?**

a) Tak, często

b) Tak, ale rzadko

c) Nie, nigdy

9. **Czy kiedykolwiek padłeś ofiarą oszustwa (lub innego przestępstwa) przez Internet lub usiłowano takiego dokonać w stosunku do Ciebie?**

a) Tak, raz

b) Tak, więcej niż raz

c) Nie, nigdy

10. **Czy kiedykolwiek ktoś z Twoich bliskich padł ofiarą oszustwa (lub innego przestępstwa) przez Internet lub usiłowano takiego dokonać?**

d) Tak, raz

e) Tak, więcej niż raz

f) Nie, nigdy

11. **Czy na skutek działania w Internecie utraciłeś mienie lub majątek?**

a) Tak

b) Nie

c) Jeśli tak jakiej wartości ….

12. **Czy korzystasz z bankowości elektronicznej?**

a) Tak

b) Nie

13. **Czy korzystasz z Internetowego Konta Pacjenta?**

a) Tak

b) Nie

14. **Czy korzystasz z platformy profilu zaufanego?**

a) Tak

b) Nie

15. **Czy korzystasz z możliwości umówienia wizyt u lekarza, w urzędach i instytucjach użyteczności publicznej przez Internet?**

a) Tak

b) Nie

16. **Czy jesteś świadomy zagrożeń wynikających z Internetu?**

a) Nie zastanawiam się nad tym

b) Tak, odpowiednio chronię swoje dane

c) Internet to moim zdaniem bezpieczne miejsce

17. Czy korzystasz z dwuskładnikowego uwierzytelniania hasła na różnych platformach?

a) Tak

b) Nie

c) Nie słyszałam/łem o takim rozwiązaniu

18. W jaki sposób najczęściej nawiązujesz kontakt z innymi ludźmi?

a) Telefon

b) Osobiste spotkanie

c) SMS,

d) Komunikatory społecznościowe: Messenger, WhatsApp, Snapchat, Instagram, Telegram, Discord.

19. Czy posiadasz konto użytkownika na portalu społecznościowym Facebook?

a) Tak

b) Nie

20. Czy posiadasz konto użytkownika na portalu społecznościowym Instagram?

c) Tak

d) Nie

21. W jaki sposób opłacasz zakupy internetowe i bieżące rachunki?

a) Przelew internetowy tradycyjny

b) BLIK

c) Płatność przy odbiorze/przelew pocztowy

22. Czy przechowujesz w pamięci swojego telefonu lub w portfelu informacje na temat numeru PIN do karty płatniczej lub danych do logowania do bankowości elektronicznej?

a) Tak

b) Nie

23. Czy w przypadku otrzymywania wiadomości na temat nieopłaconego rachunku/paczki z podaniem linka do uregulowania płatności:

a) Wchodzę w link, aby dokonać płatności

b) Weryfikuję autentyczność wiadomości

c) Ignoruję takie wiadomości

24. Czy podczas dokonywania zakupów przez Internet, np. zakupu biletów lotniczych, rezerwacji noclegów podajesz numer karty kredytowej wraz z kodem CVV oraz datą ważności?

a) Tak, nie zastanawiam się nad bezpieczeństwem transakcji

b) Tak, ale tylko na sprawdzonych stronach internetowych

c) Nigdy nie podaję

25. Czy w przypadku dokonania na Twoją szkodę oszustwa przez Internet zgłosił byś sprawę organom ścigania?

a) Tak

b) Spróbowałbym sam odzyskać utracone pieniądze

c) Nie, nie wierzę w wykrycie sprawcy i odzyskanie pieniędzy

Załącznik nr 2 – Wzór kwestionariusza ankiety udostępnionej w drugiej grupie badawczej

1. **Płeć:**
   a) Kobieta
   b) Mężczyzna
   c) Nie chcę wskazywać.
2. **Wiek:**
   a) 15 lat
   b) 16 lat
   c) 17 lat
   d) 18 lat
3. **Jak często korzystasz z Internetu w ciągu dnia?**
   a) Wcale
   b) Bardzo rzadko, tj. mniej niż 1 godzinę
   c) 2-4 godziny
   d) Powyżej 4 godzin
4. **W jakim celu przeważnie korzystasz z Internetu?** (możliwość zaznaczenia kilku odpowiedzi)
   a) Portale społecznościowe
   b) Informacje ze świata i kraju
   c) Poczta elektroniczna
   d) Opłata rachunków, załatwienie spraw
   e) Telewizja internetowa
   f) Rozrywka
   g) Nauka
5. **Za pomocą jakiego łącza korzystasz z Internetu?**
   a) Stałe łącze, sieć wifi domowa
   b) Otwarte/darmowe łącze w galeriach handlowych, pociągach, miejscach publicznych,
   c) Transmisja danych od operatora sieci komórkowej w telefonie
6. **Skąd głównie czerpiesz informacje na temat sytuacji w kraju i na świecie?**
   a) Z telewizji
   b) Z Internetu
   c) Od znajomych i współpracowników
   d) Nie interesuje się tym
7. **Czy korzystasz z platform sprzedażowych typu Olx, Otomoto, Vinted, Marketplace?**
   a) Tak, często
   b) Tak, ale rzadko
   c) Nie, nigdy

8. **Czy kiedykolwiek padłeś ofiarą oszustwa (lub innego przestępstwa) przez Internet lub usiłowano takiego dokonać w stosunku do Ciebie?**
   a) Tak, raz
   b) Tak, więcej niż raz
   c) Nie, nigdy
9. **Czy kiedykolwiek ktoś z Twoich bliskich padł ofiarą oszustwa (lub innego przestępstwa) przez Internet lub usiłowano takiego dokonać?**
   a) Tak, jednokrotnie
   b) Tak, więcej niż raz
   c) Nie, nigdy
10. **Czy na skutek działania w Internecie utraciłeś mienie lub majątek?**
   a) Tak
   b) Nie
   c) Jeśli tak jakiej wartości ….
11. **Czy korzystasz z bankowości elektronicznej?**
   a) Tak
   b) Nie
12. **Czy korzystasz z Internetowego Konta Pacjenta?**
   a) Tak
   b) Nie
13. **Czy korzystasz z platformy profilu zaufanego?**
   a) Tak
   b) Nie
14. **Czy korzystasz z możliwości umówienia wizyt u lekarza, w urzędach i instytucjach użyteczności publicznej przez Internet?**
   a) Tak
   b) Nie
15. **Czy jesteś świadomy zagrożeń wynikających z Internetu?**
   a) Nie zastanawiam się nad tym
   b) Tak, odpowiednio chronię swoje dane
   c) Internet to moim zdaniem bezpieczne miejsce
16. **Czy korzystasz z dwuskładnikowego uwierzytelniania hasła na różnych platformach?**
   a) Tak
   b) Nie
   c) Nie słyszałam/łem o takim rozwiązaniu
17. **W jaki sposób najczęściej nawiązujesz kontakt z innymi ludźmi?**
   a) Telefon
   b) Osobiste spotkanie

c) SMS,

d) Komunikatory społecznościowe: Messenger, WhatsApp, Snapchat, Instagram, Telegram, Discord.

18. **Czy posiadasz konto użytkownika na portalu społecznościowym Facebook?**

a) Tak

b) Nie

19. **Czy posiadasz konto użytkownika na portalu społecznościowym Instagram?**

a) Tak

b) Nie

20. W jaki sposób opłacasz zakupy internetowe i bieżące rachunki?

a) Przelew internetowy tradycyjny

b) BLIK

c) Płatność przy odbiorze/przelew pocztowy

21. **Czy przechowujesz w pamięci swojego telefonu lub w portfelu informacje na temat numeru PIN do karty płatniczej lub danych do logowania do bankowości elektronicznej?**

a) Tak

b) Nie

22. Czy w przypadku otrzymywania wiadomości na temat nieopłaconego rachunku/paczki z podaniem linka do uregulowania płatności:

a) Wchodzę w link, aby dokonać płatności

b) Weryfikuję autentyczność wiadomości

c) Ignoruję takie wiadomości

23. **Czy podczas dokonywania zakupów przez Internet, np. zakupu biletów lotniczych, rezerwacji noclegów podajesz numer karty kredytowej wraz z kodem CVV oraz datą ważności?**

a) Tak, nie zastanawiam się nad bezpieczeństwem transakcji

b) Tak, ale tylko na sprawdzonych stronach internetowych

c) Nigdy nie podaję.

24. Czy w przypadku dokonania na Twoją szkodę oszustwa przez Internet zgłosił byś sprawę organom ścigania?

a) Tak

b) Spróbowałbym sam odzyskać utracone pieniądze

c) Nie, nie wierzę w wykrycie sprawcy i odzyskanie utraconych pieniędzy.