Wstęp

Rozpoczynając opracowanie łączące problematykę nauk penalnych i nowoczesnych technologii, z łatwością można przywołać oczywistą dziś prawdę: w ciągu ostatnich lat nastąpił dynamiczny rozwój technologii komputerowej, a jej możliwości są dalece większe niż jeszcze dekadę temu, niosąc ze sobą równie wiele korzyści co zagrożeń. Wymowne jest, że podobne stwierdzenia otwierały opracowania naukowe już w latach 70. XX wieku. Podkreślano wówczas, że „nasze społeczeństwo szybko staje się zależne od precyzyjnych, elektronicznych maszyn obliczeniowych (...). Wraz ze wzrostem ich popularności rośnie potencjał szkód możliwych do przypadkowego lub celowego wyrządzenia za ich pomocą”[1].

Choć zaiste nie jest to niczym nowym, wstępne stwierdzenie powyższego faktu nie stanowi wyłącznie pustego zabiegu stylistycznego. Przypomina bowiem o jasnym, choć zaskakująco łatwo zapominanym procesie towarzyszącym ludzkości od wielu wieków: że rozwój i rozpowszechnienie się dowolnej nowej technologii pozostaje w ścisłym związku z wynikającymi z jej zastosowania zmianami w zachowaniach społecznych i w postrzeganiu rzeczywistości. Trzeba przy tym pamiętać, że każda nowa technologia jest sama w sobie neutralna. Jej rzeczywiste znaczenie zależy od sposobu jej implementacji i faktycznego wykorzystania. Istnieją technologie w swych zastosowaniach na tyle nowatorskie, że zmieniające krajobraz społeczny. Odnosi się to w takim samym stopniu do przełomowych technologii współcześnie, jak i w przeszłości. Tak jak kilkadziesiąt lat po wynalezieniu prasy drukarskiej Europa nie była „starą Europą z dodaną prasą drukarską”, lecz zupełnie nową przestrzenią społeczną[2], tak też dziś świat ulega

[1] D.B. Parker, *Crime by computer*, New York 1976, s. ix.

[2] N. Postman, *Technopol. Triumf techniki nad kulturą*, przeł. A. Tanalska-Dulęba, Warszawa 2004, s. 31.

głębokim zmianom w związku z „pojawieniem się" komputerów i Internetu. Proces daleko idących zmian społecznych spowodowany wdrożeniem nowych technologii jest zjawiskiem znanym ludzkości z historii i nie powinien budzić zdziwienia.

Rzeczywiście, w ciągu ostatnich kilkudziesięciu lat sprzęt, rozwiązania informatyczne i zakres ich zastosowania przeszły niezwykle szybką ewolucję, trwale wkraczając w prywatne, zawodowe i publiczne życie społeczeństwa. Nie wymaga to obecnie potwierdzenia i poparcia poprzez przytoczenie najnowszych danych statystycznych czy rozszerzonej listy przykładów. Jest to zgodnym ze wskazaniami doświadczenia życiowego, powszechnie znanym dziś faktem.

Obecnie dokonuje się czwarta już fala nowożytnych zmian technologicznych: od pierwszej rewolucji przemysłowej w XVIII wieku, poprzez zmiany wynikające z elektryfikacji, budowę pierwszych komputerów, aż po współczesny „przemysł 4.0", oparty na rozwoju takich technologii, jak: sztuczna inteligencja, chmury obliczeniowe, Internet rzeczy czy *big data*. Pojęcie „przemysłu 4.0", rozumianego jako wyraz czwartej fali rewolucji technologicznej, wykorzystano po raz pierwszy w 2011 r. na targach technologicznych w Hanowerze podczas prezentacji założeń rządu niemieckiego odnośnie do strategii rozwoju technologii[3]. Zgodnie z jego założeniami postępująca automatyzacja metod rozwiązywania wszelkiego rodzaju problemów i dostarczania usług oparta jest coraz częściej na komunikacji pomiędzy samymi urządzeniami – bez świadomego udziału człowieka lub z jego jedynie minimalnym udziałem jako użytkownika i beneficjenta końcowego[4].

Wiele aspektów nowoczesnych technologii postrzeganych jest jako mające pozytywny wpływ na funkcjonowanie społeczeństwa, a przykłady tego rodzaju można wskazywać bez najmniejszego wysiłku: od przechowywania i udostępniania danych w formie cyfrowej, poprzez pocztę elektroniczną, po najnowocześniejsze formy dystrybucji treści i usług. Współczesne możliwości komunikacyjne, obliczeniowe, twórcze i poznawcze człowieka zostały poszerzone na niespotykaną w historii skalę. Oferta nowych rozwiązań technologicznych pozwoliła na przenoszenie „do świata cyfrowego" różnych, znanych od wieków, form ludzkiej aktywności: handlu, komunikacji czy rozrywki. Niedawny postęp był na tyle szybki, że mimo jego ewolucyjnego charakteru może być postrzegany jako skokowy. Transfer aktywności społecznej do przestrzeni cyfrowej w ostatnim czasie ulegał jedynie przyspieszeniu w efekcie wydarzeń bieżących – w marcu 2020 r., w związku z zagrożeniem

[3] M. Różycki, *Ubranie podłączone do Internetu*, „Koncept" 2018, nr 63, s. 7.

[4] M. Hermann, T. Pentek, B. Otto, *Design principles for Industrie 4.0 scenarios*, 2016 49th Hawaii International Conference on System Sciences (HICSS), 5–8 stycznia 2016 r., https://ieeexplore.ieee.org/document/7427673, dostęp 19 czerwca 2020 r.

epidemiologicznym, w systemie „pracy zdalnej" (za pośrednictwem Internetu) wykonywało swoje zadania pracownicze 17% zatrudnionych w Polsce[5].

Wzajemna relacja człowieka i technologii jest jednak trudna do jednoznacznego sklasyfikowania i scharakteryzowania. Niewykluczone, że zachwyt nad nowymi możliwościami spowodował, że nie dostrzeżono potrzeby zachowania ostrożności i rozwagi w ich wdrażaniu i stosowaniu. Technologia ma, i to z całą pewnością, bezpośredni wpływ chociażby na stosowany przez nas język, ale także na rozumienie pojęć i postrzeganie rzeczywistości[6]. Powoduje to, że w często nieuświadomiony przez nas sposób rozwój technologii wpływa na rozwój samej ludzkości. Środki techniczne, zaprojektowane początkowo jako narzędzia komunikacji, nie są dziś już tylko kanałami komunikowania się, lecz coraz częściej systemowo wpływają na relacje międzyludzkie, które kształtują się w oparciu o nową infrastrukturę. Niestety, wielokrotnie zamiast przyczyniać się w ten sposób do budowy i rozwoju społeczności – technologia osłabia rzeczywiste więzi, tworząc jedynie iluzję wspólnoty[7]. Dostrzegalny jest zatem nie tylko proces przenoszenia ludzkiej aktywności do „cyberprzestrzeni", lecz także bezpośredni wpływ tej ostatniej na świat rzeczywisty[8]. Wykorzystywanie współczesnej struktury przekazów informacyjnych w Internecie powoduje też, że sytuacja epidemiologiczna wiosną 2020 r. stanowiła jednocześnie zagrożenie dla zdrowia publicznego, jak i dla szeroko rozumianego bezpieczeństwa obrotu informacji[9]. Świat cyfrowy wpływa na ten fizyczny również w najbardziej dosłownej formie: w oparciu o technologie komputerowe zarządzamy otaczającą nas fizyczną infrastrukturą, procesami produkcyjnymi, logistycznymi, pracą, rozrywką, leczeniem.

---

[5] Według badania przeprowadzonego w dniach 23–25 marca 2020 r.; GFK, *Połowa respondentów (51%) deklaruje, że chodzi do pracy jak zwykle*, Komunikat Prasowy GFK z 26 marca 2020 r., https://www.gfk.com/pl/aktualnosci/press-release/polowa-respondentow-51-proc-deklaruje-ze-chodzi-do-pracy-jak-zwykle/, dostęp 19 czerwca 2020 r.

[6] M. Maciołek, *Promieniowanie K (komputerowe), czyli o oddziaływaniu rzeczywistości informatycznej na polszczyznę*, „Postscriptum Polonistyczne" 2017, nr 1(19), https://www.academia.edu/38117474/Promieniowanie_K_komputerowe_czyli_o_oddzia%C5%82ywaniu_rzeczywisto%C5%9Bci_informatycznej_na_polszczyzn%C4%99?email_work_card=title, dostęp 19 czerwca 2020 r.

[7] K. Szymielewicz, *Czy Internet w ogóle jeszcze służy ludziom? Pora się obudzić*, „Polityka" z 27 kwietnia 2019 r., https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1790518,1,czy-internet-w-ogole-jeszcze-sluzy-ludziom-pora-sie-obudzic.read, dostęp 19 czerwca 2020 r.

[8] Podobnie o „kręgu wzajemnego oddziaływania technologii i społeczeństwa" lub o „wzajemnym oddziaływaniu determinizmu technologicznego i społecznego" wypowiadają się m.in.: S. Vannoy, P. Palvia, *The social influence model of technology adoption*, „Communications of the ACM" 2010, nr 53(6), s. 150; P. Wiśniewski, J. Boehlke, *Cyberprzestępczość w gospodarce*, Toruń 2017, s. 68–69.

[9] K. Gradoń, *Crime in the time of the plague: fake news pandemic and the challenges to law enforcement and Intelligence community*, „Society Register" 2020, nr 4(2), s. 133–148.

Długofalowe konsekwencje tego rodzaju konwergencji są trudne do przewidzenia, a ich pogłębiona ocena na gruncie filozoficznym pozostaje poza zakresem niniejszego opracowania. Pytania te pozostają więc otwarte. Z całą pewnością jednak stały rozwój wymaga równie stałej adaptacji, umiejętności dostrzegania nowych zagrożeń i reagowania na nie.

Zmiany technologiczno-społeczne mają oczywisty i bezpośredni wpływ na sferę prawnie relewantną, w tym na obszary związane z szeroko rozumianym wymiarem sprawiedliwości i na nauki penalne, na prawo i postępowanie karne oraz potrzeby i możliwości technik kryminalistycznych. Widocznym i wpływającym na codzienność skutkiem przenoszenia działalności ludzkiej do „świata cyfrowego" oraz oddziaływań odwrotnych jest rozwój różnorodnych negatywnych zjawisk społecznych, związanych – mniej lub bardziej ściśle – z wykorzystaniem urządzeń komputerowych i sieci teleinformatycznych. Zjawisko określone u progu jego powstania jako „przestępczość komputerowa" (a dziś określane chętniej mianem „cyberprzestępczości") ewoluowało i zmieniało się wraz z rozwojem technologii.

Stopniowo pojawiały się zarówno całkowicie nowe formy zachowań szkodliwych, wymagające niekiedy interwencji legislacyjnych, jak i po prostu nowe sposoby popełniania „tradycyjnych" czynów zabronionych. Centralna rola, jaką zdobyły nowe technologie w życiu człowieka, nie jest bezpośrednim źródłem tych problemów, lecz zdecydowanie przyczynia się do szczególnie intensywnego wzrostu częstotliwości ich występowania i szkodliwości społecznej. Sprzęt komputerowy należy współcześnie do standardowych wręcz narzędzi wykorzystywanych przez sprawców bardzo różnych typów czynów zabronionych – zarówno jako konieczny element *modus operandi*, jak i jedynie pomocniczo. Przekłada się to na nowe wyzwania dla nauk penalnych, nie tylko w kontekście materialnego prawa karnego, lecz także (a może przede wszystkim) w zakresie postępowania dowodowego i kryminalistyki.

Czynności dowodowe w postępowaniach dotyczących czynów popełnianych w związku z wykorzystaniem komputerów często wymagają, co oczywiste, pozyskania i analizy informacji wynikających z danych cyfrowych. Praktyczny zakres pojęcia „dowód cyfrowy" jest bardzo szeroki, obejmuje bowiem zarówno materiał związany z czynami wysoce wyspecjalizowanymi, popełnionymi z użyciem zaawansowanych technik informatycznych, jak i wszystkie inne materiały cyfrowe generowane w kontekście typów czynów zabronionych popełnianych powszechnie, przez osoby o relatywnie niskim poziomie kwalifikacji technicznych. Nie ulega wątpliwości, że znaczenie materiałów cyfrowych w sferze prawnej stale wzrasta, a „dowodem cyfrowym" jest praktycznie każda treść generowana w związku z funkcjonowaniem komputerów. Wiadomości elektroniczne, materiały pochodzące z wewnętrznych systemów przetwarzania danych, pliki tekstowe, graficzne czy dźwiękowe,

zawartości stron internetowych i wszelkie inne dane przetwarzane i przechowywane w formie cyfrowej coraz częściej są istotnymi elementami materiału dowodowego w sprawach karnych.

Wiele opracowań dotyczących problemów informatycznych w kontekście kryminalistyki skupionych jest na realizacji czynności dochodzeniowo-śledczych. Informatyka kryminalistyczna (czy też: śledcza, sądowa) w popularnym odbiorze stanowi między innymi zespół technik umożliwiających rekonstrukcję przebiegu zdarzenia o ściśle technicznym charakterze. A jednak należy pamiętać, że upowszechnienie się narzędzi cyfrowych i ich wykorzystania w obrocie społeczno-gospodarczym powoduje występowanie śladów cyfrowych w wielu rodzajach spraw karnych, niekojarzonych wcześniej z technologią. Zasadne jest zatem pytanie o prawidłowe sposoby postrzegania, pozyskiwania czy oceny różnych materiałów pochodzenia cyfrowego – choćby w sprawach błahych, prostych z punktu widzenia eksperta z zakresu informatyki. W ten bowiem sposób, między innymi, realizuje się dowodowa funkcja kryminalistyki.

Fundamentalna zasada dążenia do ustalenia w toku postępowania karnego prawdy materialnej nakłada na organy procesowe obowiązek realizacji czynności i oceny materiału dowodowego w zgodzie ze „wskazaniami wiedzy" – rekonstruowanymi na podstawie adekwatnych opracowań naukowych. Przyjmując założenie, że należy poważnie traktować zasady procesu karnego, w tym w szczególności wynikającą zarówno z ustawy procesowej[10], jak i z norm rangi konstytucyjnej zasadę domniemania niewinności i rozstrzygania wątpliwości na korzyść oskarżonego – procesowe wykorzystanie materiałów pochodzenia cyfrowego musi opierać się na możliwych do zweryfikowania i naukowych podstawach kryminalistycznych.

Z kryminalistycznego punktu widzenia podstawowym kryterium oceny materiałów cyfrowych powinna być ich wiarygodność techniczna – dopiero w dalszej kolejności ocenie powinno podlegać znaczenie ich treści w kontekście prowadzonego postępowania. Dla zapewnienia wspomnianej wiarygodności konieczne jest natomiast, jak słusznie stwierdził Sąd Najwyższy w wyroku z 20 czerwca 2013 r. (sygn. III KK 12/13), stosowanie się do zasad wypracowanych na gruncie informatyki kryminalistycznej[11]. To ta dziedzina dostarcza naukowo uzasadnionych technik i taktyk postępowania z cyfrowym materiałem dowodowym. Przyjmując, że „dowodem cyfrowym" jest faktycznie każda (istotna dowodowo) informacja mająca postać danych cyfrowych, a jego zabezpieczenie z zachowaniem wiarygodności wymaga

[10] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2020 r. poz. 30 ze zm.), dalej: kpk, ustawa procesowa.

[11] Wyrok Sądu Najwyższego z 20 czerwca 2013 r., sygn. III KK 12/13, Biuletyn Prawa Karnego 2013, nr 8, s. 11.

zastosowania odpowiednich do tego narzędzi wypracowanych na gruncie informatyki kryminalistycznej – należałoby oczekiwać takich działań wobec materiałów pochodzenia cyfrowego we wszystkich sprawach karnych. Powinno mieć to miejsce niezależnie od tego, czy zarzucany czyn polegał na włamaniu do systemu informatycznego, oszustwie dokonanym poprzez internetową platformę sprzedażową czy na publikacji niedozwolonych treści w mediach społecznościowych. W konsekwencji oczywista wydaje się potrzeba istnienia (i przestrzegania) odpowiednich procedur postępowania z danymi i nośnikami danych cyfrowych, które mogą stanowić dowód. Potrzeba ustalania i przestrzegania kryminalistycznych i procesowych reguł postępowania wobec określonego rodzaju materiału dowodowego wydaje się postulatem wręcz trywialnym.

Pomimo istniejących już publikacji dotykających problematyki dowodów cyfrowych trudno uznać przedmiotowe zagadnienie za wyczerpująco opisane – w szczególności bowiem w znacznym stopniu niezbadana pozostaje rzeczywista praktyka odnośnie do pozyskiwania cyfrowego materiału dowodowego i posługiwania się nim w postępowaniu karnym. Informacje naukowe dotyczące „przestępstw komputerowych" czy dowodu cyfrowego obejmują najczęściej – co oczywiście również przydatne – opracowania teoretyczne oraz przedstawiające przykłady ilustrujące potencjalne problemy i zagrożenia. Przegląd i analiza dotychczasowych opracowań pozwalają na przedstawienie hipotetycznego opisu „poprawnego naukowo" sposobu postępowania wobec dowodu cyfrowego. Nieznany pozostaje jednak zakres zgodności pomiędzy wskazaniami teorii a praktyką.

Główny problem badawczy podjęty w niniejszym opracowaniu, rozumiany jako stan obiektywnej niewiedzy określony na gruncie wiedzy dotychczasowej[12], stanowi informacja o praktyce współczesnych postępowań karnych w sprawach przestępstw, w których występują dowody cyfrowe. W szczególności zaś celowe jest ustalenie obrazu rzeczywistej praktyki w zderzeniu z poprawnymi metodami wykorzystywania takich dowodów postulowanymi w kryminalistyce i nauce procesu karnego. Problem ten jest rozstrzygalny empirycznie, a ograniczenie pola niewiedzy w tym zakresie umożliwi przedstawienie adekwatnych wniosków w warstwie zarówno teoretycznej, jak i praktycznej – nadając jego rozstrzygnięciu walor przydatności[13].

---

[12] J. Apanowicz, *Metodologia ogólna*, Gdynia 2002, s. 44–45. Por. J. Sztumski, *Wstęp do metod i technik badań społecznych*, Katowice 2010, s. 46.

[13] Cele poznawcze oraz praktyczne prowadzonych badań naukowych są ściśle powiązane ze sobą; J. Stochaj, Ł. Roman, *Wybrane metody teoretyczne w naukach społecznych i ich zastosowanie*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia AON" 2013, nr 2(6), s. 181. Por. M. Łobocki, *Metody i techniki badań pedagogicznych*, Kraków 2011, s. 25.

Bezpośrednim celem niniejszego opracowania jest zatem ustalenie, do jakiego stopnia wytyczne naukowe, wynikające z wiedzy kryminalistycznej opisującej posługiwanie się dowodami cyfrowymi, są uwzględniane i realizowane w rzeczywistej praktyce sądowej polskiego postępowania karnego. Logiczną konsekwencją tak postawionego celu ogólnego jest także cel szczegółowy: przedstawienie wniosków co do różnych aspektów wykorzystania dowodów cyfrowych zarówno w teorii kryminalistyki i procesu karnego, jak i w wymiarze praktycznego stosowania prawa. Wpisuje się to w realizację poznawczej funkcji badań naukowych (poprzez zbadanie i wyjaśnienie wskazanych zagadnień) oraz ich funkcji praktycznej (pozwalając na wykorzystanie zgromadzonej wiedzy w celu wzbogacenia i zmiany praktyki, m.in. poprzez wskazanie postulatów zmian legislacyjnych)[14]. Wstępny przegląd literatury przedmiotu oraz dotychczasowa bezpośrednia obserwacja praktyki sądowej wskazują, że w odniesieniu do powyższego problemu uzasadnione jest sformułowanie następujących hipotez[15], które zostaną rozwinięte, uzasadnione i zweryfikowane w toku niniejszej pracy.

Po pierwsze, wykorzystywanie przez sprawców komputerów i Internetu w związku z popełnianymi czynami zabronionymi jest powszechne. Dotyczy to także przestępstw niezwiązanych ściśle z systemami informatycznymi, których popełnienie byłoby możliwe również bez udziału technologii (takich jak np. oszustwo czy naruszenia praw autorskich). Prostą tego konsekwencją jest nie mniej powszechne występowanie w sprawach karnych szeroko rozumianych dowodów cyfrowych: wiadomości elektronicznych, informacji z systemów przetwarzania danych, treści stron internetowych, zawartości plików różnego typu i wielu innych.

Po drugie, w większości spraw, w których występują dowody cyfrowe, nie zabezpiecza się ich bezpośrednio w ramach działań organów ścigania i nie bada w sposób zgodny z wytycznymi informatyki kryminalistycznej. Materiały tego typu podlegają przeważnie analizie treściowej (nie technicznej) na podstawie ich wydruków, nierzadko dostarczanych przez osoby zainteresowane wynikiem postępowania. Innymi słowy: w większości przypadków technik wypracowanych przez informatykę kryminalistyczną w ogóle się nie stosuje. Przyjmowana w teorii kryminalistyki definicja „dowodu cyfrowego" kształtowana w końcu XX wieku jest obecnie nadmiernie szeroka, co powoduje rozdźwięk pomiędzy teorią a praktyką procesu karnego. Sposób postrzegania i zakres pojęcia dowodu cyfrowego w postępowaniu

[14] J. Stochaj, Ł. Roman, *Wybrane metody…*, s. 180–181.

[15] Przyjmując, że hipoteza badawcza oznacza świadomie przyjęte przypuszczenie, wywiedzione z dotychczasowych obserwacji i doświadczeń, gdzie w oparciu o fakty znane i dostatecznie sprawdzone można przypuszczać o kształcie badanego zjawiska. Zob. M. Łobocki, *Metody…*, s. 27; J. Apanowicz, *Metodologia…*, s. 47–48.

karnym wymaga rewizji i aktualizacji w kontekście zmian społecznych i technologicznych ostatnich dziesięcioleci.

Po trzecie, niezależnie od istniejących w praktyce niedociągnięć wiarygodność dowodów cyfrowych jest bardzo rzadko kwestionowana przez uczestników postępowania. Sprzeciwu stron (w tym oskarżonych) nie budzi na ogół posługiwanie się w charakterze dowodów, łatwo przecież poddającymi się falsyfikacji, wydrukami treści cyfrowych. Uczestnicy postępowań karnych, nawet gdy zaprzeczają znaczeniu treści dowodów cyfrowych, najczęściej nie podważają ich wiarygodności.

Po czwarte, nawet podniesienie przez stronę zarzutu niewiarygodności dowodu cyfrowego (spowodowanej np. niedochowaniem zasad informatyki kryminalistycznej) na ogół nie stoi na przeszkodzie uznaniu dowodu przez organ sądowy za wiarygodny. Ponieważ jednak techniki informatyki kryminalistycznej mają, w zamierzeniu, gwarantować naukową wiarygodność dowodów cyfrowych, należy rozważyć, czy odstąpienie od ich stosowania nie uderza w realizację zasad postępowania karnego.

Po piąte, obecne regulacje dotyczące gromadzenia i przeprowadzania dowodów nie dostarczają jednoznacznych, skutecznych i stosunkowo uniwersalnych podstaw prawnych służących pozyskiwaniu dowodów cyfrowych. Aktualnie obowiązujące przepisy nakazują co do zasady, aby wobec danych cyfrowych stosować „odpowiednio" przepisy projektowane w przeszłości z myślą o świecie rzeczywistym (np. przeszukanie i zatrzymanie rzeczy). Takie podejście nie jest obecnie wystarczające. Różnorodność stanów faktycznych, rodzajów danych przydatnych dowodowo, ich źródeł i podmiotów je przetwarzających powoduje, że w niektórych przypadkach obowiązujące przepisy w ogóle nie dostarczają koniecznym działaniom organów ścigania adekwatnych podstaw prawnych. Sprzyja to także niejednolitemu, chaotycznemu stosowaniu istniejących norm – ze szkodą dla jakości stosowania prawa. W tym kontekście szczególnie uzasadnione może być podniesienie postulatów zmian legislacyjnych.

Weryfikacja przedstawionych hipotez wymaga podjęcia badań zarówno teoretycznych, jak i empirycznych, co odzwierciedla również poznawczo-praktyczny charakter zarysowanych problemów[16]. Niezbędna jest zatem informacja o metodologii niniejszej pracy. Badania teoretyczne mają w znacznej mierze charakter wtórny – odwołują się wszak do analizy źródeł dotychczas zgromadzonej wiedzy. Pozwalają jednak na usystematyzowanie jej i ocenę z uaktualnionej perspektywy, a także na dokonanie niezbędnych uogólnień, umożliwiających realizację dalszych, empirycznych zamie-

[16] J. Kawa, *Metodologia, metodyka, metoda jako podstawa wywodu naukowego*, „Studia Prawnoustrojowe" 2013, nr 21, s. 177–178; J. Stochaj, Ł. Roman, *Wybrane metody…*, s. 181.

rzeń badawczych. W kontekście dowodów cyfrowych niezbędne jest przy tym, nieodzowne dla kryminalistyki, podejście interdyscyplinarne, łączące wiedzę prawniczą i techniczną w oparciu o podstawowe, komplementarne metody i techniki badawcze[17], bazujące na analitycznych i syntetycznych sposobach rozumowania[18].

W toku rozważań teoretycznych oczywiste zastosowanie znalazła metoda analizy i krytyki źródeł oraz piśmiennictwa, której istota polega na wskazaniu odrębności i oryginalności podjętych problemów na tle dotychczasowego stanu wiedzy. Przeprowadzone i opisane tu badania literaturowe obejmują możliwie pełen zakres dostępnej, w szczególności polskiej i anglojęzycznej, literatury technicznej, prawniczej oraz informacji z innych źródeł otwartych odnoszących się w swej treści do badanych zagadnień. Pozwoli to na wyodrębnienie istotnych cech badanych zagadnień do celów dalszych analiz. Zastosowanie tej metody jest istotne zwłaszcza przy próbie rekonstrukcji naukowo poprawnych metod działań zalecanych w ramach informatyki kryminalistycznej. Należy przy tym wskazać, że wobec braku formalnych procedur dotyczących posługiwania się dowodami cyfrowymi większość dotychczasowych rozważań tego dotyczących została przedstawiona właśnie w literaturze przedmiotu (w szczególności anglojęzycznej).

Szerokie zastosowanie znajduje także metoda analizy porównawczej (prawnej i doktrynalnej), która jest pochodną metody analizy i krytyki źródeł zmierzającą do stwierdzania zależności jednych zjawisk i wytworów działalności ludzkiej od drugich[19]. Analiza porównawcza stanowiła istotny element rozważań prowadzonych nad zagadnieniami definicyjnymi. Niezbędna była również w toku rozważań ściśle merytorycznych, pozwalając na ujawnianie zależności występujących w badanych źródłach odnoszących się do tych samych zagadnień.

W pewnym zakresie zastosowanie znalazła też metoda historyczna (historyczno-opisowa, historyczno-prawna), którą współcześnie należy pojmować jako stanowisko poznawcze orientujące się na wyjaśnienie

[17] Rozumiane tu odpowiednio jako: systematycznie stosowane sposoby postępowania, na które składają się czynności myślowe i praktyczne oraz skonkretyzowane sposoby realizowania tych zamierzeń. W tym znaczeniu „techniki" badawcze stanowią kategorię podrzędną wobec „metod", które skupiają się na opisie teoretycznego sposobu rozumowania. Ścisłe rozróżnienie metod oraz technik badawczych budzi jednak kontrowersje i nie wydaje się niezbędne dla prawidłowego przebiegu rozumowania w obszarze nauk społecznych. Zob. W. Okoń, *Nowy słownik pedagogiczny*, Warszawa 2004, s. 328. Por. T. Kotarbiński, *Elementy teorii poznania, logiki formalnej i metodologii nauk*, Wrocław 1990; M. Łobocki, *Metody*…, s. 115.

[18] Należy pamiętać, że w procesie badawczym analiza występuje i wzajemnie wiąże się z syntezą, warunkując ją. Synteza zaś może stanowić punkt wyjścia do kolejnych analiz. J. Stochaj, Ł. Roman, *Wybrane metody*…, s. 184.

[19] J. Apanowicz, *Metodologia*…, s. 72.

rzeczywistości z uwzględnieniem jej genezy i tendencji rozwojowych przejawiających się w czasie i przestrzeni. Chodzi zatem o rozpatrywanie zjawisk i procesów istotnych badawczo przez pryzmat uwarunkowań dziejowych[20]. Okoliczności historyczne mają niezwykle istotny wpływ na sposób postrzegania współczesnych pojęć i terminów – jest to wyraźnie dostrzegalne w odniesieniu do przestępczości komputerowej i dowodów cyfrowych. Uwzględnienie procesów historycznych związanych z rozwojem technologii dostarcza niezbędnego kontekstu i pozwala na pogłębienie rozważań nad współczesnością. Ma to niebagatelne znaczenie dla dokonanej w niniejszej pracy rewizji przyjmowanych definicji i stanowisk teoretycznych.

Niezwykle istotne dla opisu procesowych metod wykorzystywania danych cyfrowych w postępowaniu karnym jest badanie źródeł prawa. Analizy tekstów aktów normatywnych zostały przeprowadzone z zastosowaniem metody formalno-dogmatycznej[21] i na podstawie adekwatnych reguł wykładni i interpretacji przepisów znanych prawoznawstwu[22]. W szczególności uwzględniono związane z badaną tematyką przepisy prawa międzynarodowego, ustawy procesowej i innych ustaw, rozporządzeń oraz aktów prawa wewnętrznego obowiązującego w Polsce, jak również niektóre normy zagraniczne. Dzięki temu możliwe będzie zidentyfikowanie sytuacji problemowych z punktu widzenia obowiązującego prawa i przedstawienie postulatów zmian w legislacji.

Oczywiście, wszelkie prowadzone analizy źródeł (czy to literaturowych, normatywnych, czy innych) prowadzone będą *de facto* w oparciu o metodę badań dokumentów, która polega na gromadzeniu, selekcji, opisie i naukowej interpretacji faktów[23] wynikających z ich treści. Badanie dokumentów, postrzegane również w węższym rozumieniu jako technika badawcza, pozwala na uwzględnienie bardzo szerokiego zakresu wytworów ludzkich, gdyż dokumentem podlegającym badaniu może być każdy przedmiot materialny wyrażający myśl, osiągnięcie czy propozycję. Obejmuje to zatem pozycje literaturowe, treść artykułów i doniesień (również medialnych), ale także akty normatywne, orzecznictwo, regulaminy, raporty, zbiory danych statystycznych, publikowane treści zaleceń i wytycznych oraz wszelkie inne źródła.

---

[20] P. Dobosz, *Problemy metodologii współczesnej nauki prawa administracyjnego na tle metody historyczno-prawnej*, „Kwartalnik Prawa Publicznego" 2001, nr 1(1), s. 31–32.

[21] R. Tokarczyk, *Komparatystyka prawnicza*, Warszawa 2008, s. 76.

[22] M. Zieliński, *Wykładnia prawa. Zasady – reguły – wskazówki*, Warszawa 2017, s. 43–57.

[23] J. Apanowicz, *Metodologia…*, s. 68–69, 90; A. Mróz-Jagiełło, A. Wolanin, *Metoda analizy i krytyki dokumentów w naukach o bezpieczeństwie*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia AON" 2013, nr 2(6), s. 113–115.

Badanie empiryczne opisane w niniejszej pracy przeprowadzono z wykorzystaniem analizy aktowej dokonanej metodą badań statystycznych[24]. Celem badania prowadzonego metodą analizy aktowej jest, zgodnie z celem ogólnym pracy, ograniczenie pola niewiedzy w zakresie praktyki posługiwania się materiałem dowodowym pochodzenia cyfrowego w postępowaniu karnym. Badana populacja obejmuje akta postępowań karnych prawomocnie zakończonych w latach 2016–2018 w sądach rejonowych leżących we właściwości Sądu Okręgowego w Warszawie, prowadzonych w kierunku wybranych kwalifikacji prawnych. Ograniczenie badania aktowego do spraw przeprowadzonych w ciągu tych trzech lat miało na celu ustalenie obrazu względnie aktualnych praktyk, związanych z obecnym stanem rozwoju prawa i technologii. Prawomocne zakończenie postępowania jest zaś warunkiem uzyskania wiadomości o ostatecznej i wiążącej ocenie materiału dowodowego w danej sprawie.

Warto podkreślić, że głównym celem badania będzie poznanie określonych jakościowo elementów rzeczywistości postępowań w zakresie wykorzystania dowodów cyfrowych, a nie ustalenie częstotliwości ich występowania w sprawowaniu wymiaru sprawiedliwości w ogóle. Z tego też powodu uwzględniono próbę badawczą o ograniczonej reprezentatywności. Dobór kwalifikacji prawnych spraw objętych badaniem był podyktowany względami celowościowymi – oczekiwaniem, że wskazane typy czynów zabronionych mogą się wiązać z występowaniem istotnego badawczo cyfrowego materiału dowodowego. Wyboru konkretnych akt postępowań w ramach tak określonej populacji (N) dokonano zaś z uwzględnieniem wszystkich postępowań w sprawach czynów zabronionych rzadziej występujących w praktyce (dla których $N<100$), a w pozostałym zakresie – z zastosowaniem probabilistycznej (losowej) metody doboru akt. Badana próba ($n = 370$) składa się zatem z postępowań kwalifikowanych z różnych przepisów karnych i ma charakter częściowo reprezentatywny, co jednak nie zaprzecza ich wartości, biorąc pod uwagę jakościowy charakter wielu zmiennych oraz cel prowadzonych badań[25].

W wymiarze redakcyjnym zaś wewnętrzna systematyka niniejszej publikacji zakłada stopniowe przejście od omówienia zagadnień teoretycznych do opisu praktyki wykorzystywania dowodów cyfrowych w polskim postępowaniu karnym.

Rozdział pierwszy dotyczy bezpośrednio „dowodu cyfrowego" jako pojęcia jednocześnie prawnego i technicznego. W celu ujednolicenia zagadnień

[24] Niezbędnej przy gromadzeniu, porządkowaniu oraz wyciąganiu wniosków na podstawie wyodrębnionych cech elementów zbiorów danych. Por. J. Apanowicz, *Metodologia*…, s. 74–76.

[25] Por. J. Kawa, *Metodologia*…, s. 179.

terminologicznych zaproponowano we wstępnej jego części, sformułowane z perspektywy kryminalistyczno-dowodowej, definicje przestępczości komputerowej oraz cyberprzestępczości. Następnie przedstawiona została podstawowa wiedza o zjawiskach fizycznych oraz zagadnieniach informatycznych kryjących się pod pojęciem „dane w formie cyfrowej". Dowody cyfrowe zostały umiejscowione w ramach tradycyjnych klasyfikacji śladów i dowodów w sposób uwzględniający ich specyficzne cechy. Zarazem definicja dowodu cyfrowego przyjmowana dotychczas w teorii kryminalistyki została poddana gruntownej rewizji z perspektywy końca drugiej dekady XXI wieku. Proponowana zaktualizowana i ujednolicona definicja klasyfikacyjna obejmuje rozróżnienie sposobu postrzegania dowodowych treści pochodzenia cyfrowego w znaczeniu szerokim (*sensu largo*) oraz kryminalistycznym (*sensu stricto*). Wprowadzenie takiego rozróżnienia ma konsekwencje praktyczne i znajduje uzasadnienie we współczesnym sposobie postrzegania technologii cyfrowych na sali sądowej.

Rozdział drugi stanowi rezultat analizy źródeł obowiązującego w Polsce prawa dotyczącego pozyskiwania treści pochodzenia cyfrowego dla celów dowodowych w postępowaniu karnym. Zawiera zatem podsumowanie, omówienie i ocenę procesowych instrumentów gromadzenia dowodów cyfrowych, w tym czynności procesowych temu służących. Procesowe aspekty pozyskiwania dowodów cyfrowych nie są wolne ani od problemów interpretacyjnych i faktycznych, ani od błędów legislacyjnych. Dynamiczny rozwój technologii powoduje też ich częściową nieprzydatność – rzeczywista skuteczność i poprawność stosowania niektórych narzędzi procesowych doznają istotnych ograniczeń w wyniku zmian w sposobie przetwarzania, przechowywania i wykorzystywania danych cyfrowych. Przeprowadzone analizy prawne pozwalają na przedstawienie konkretnych postulatów ustawodawczych.

W rozdziale trzecim problem procesowego zabezpieczania dowodów cyfrowych został omówiony z perspektywy technik i taktyk kryminalistycznych. W ciągu wielu ostatnich lat sformułowano na gruncie informatyki kryminalistycznej szereg zasad oraz praktycznych metod postępowania. Pomimo licznych prób nie istnieje jednolita, powszechnie akceptowana czy też prawnie wiążąca metodyka postępowania z dowodami cyfrowymi. Oczekiwanie na jej stworzenie, w obliczu stale ewoluującej różnorodności technologicznej, jest zarazem nieracjonalne. Z perspektywy procesowej brak uniwersalnie akceptowanych metod utrudnia dokonanie sądowej oceny wartości takich dowodów według kryteriów naukowych. Istnieje jednak wiele wytycznych merytorycznych o podstawowym charakterze, których przestrzeganie powinno zapewnić wiarygodność i przydatność dowodową zabezpieczanych materiałów. Te tzw. zasady podstawowe informatyki kryminalistycznej mogą służyć jako względnie uniwersalna podstawa do formułowania ocen wiarygodności dowodów cyfrowych w procedurze sądowej.

Zgromadzona w ten sposób wiedza posłuży, zgodnie z zasadniczym celem niniejszego opracowania, zbadaniu i opisaniu obrazu rzeczywistego wykorzystania materiałów pochodzenia cyfrowego w praktyce sądowej. Opis badań, zawarty w rozdziale czwartym, obejmuje sprawozdanie z przeprowadzonych analiz aktowych oraz omówienie ich wyników. Pozwala to na weryfikację przedstawionych hipotez odnośnie do procesowej i kryminalistycznej poprawności posługiwania się dowodami cyfrowymi w postępowaniu karnym.

Przedstawione rozważania, także techniczne, prowadzone są ze szczególnym uwzględnieniem perspektywy przedstawicieli zawodów prawniczych – dlatego nie obejmują pogłębionych analiz technicznych właściwych naukom informatycznym, choć uwzględniają je w niezbędnym zakresie. Niniejsza publikacja jest zatem kierowana do wszystkich tych, którzy w kontekście wykonywanych zawodów prawniczych lub zainteresowań badawczych pragną pogłębić swoją wiedzę na temat teoretycznych oraz praktycznych aspektów kryminalistyczno-procesowego wykorzystywania dowodów cyfrowych w polskim postępowaniu karnym.