Nowoczesny e-proces karny. Między teraźniejszością a przyszłością

Fragment

Rozdział III. Specyfika dowodu cyfrowego w postępowaniu karnym

dr Paweł Czarnecki

§ 1. Wprowadzenie

Wypowiadając się o procesie karnym – czy to w czasie debaty, czy też w piśmiennictwie, można spotkać rozmaite porównania, figury stylistyczne lub metafory, które mają przybliżyć odbiorcom skomplikowaną materię, jaką ma określać byt zwany procesem karnym. Proces karny ujmowany jako ciąg dynamiczny czynności procesowych podobny jest do sztuki teatralnej, meczu piłkarskiego, gry ulicznej, potrawy kulinarnej czy układanki z puzzlami czy osi czasu. Badając jednak zarówno cele, jak i przedmiot procesu karnego, wydaje się, że przypomina on majestatyczny drapacz chmur, bowiem podobnie jak wskazana budowla powstała na podstawie planu architektonicznego (ustawodawca i ustrojodawca) składa się z wielu pięter (stadiów i etapów procesowych), przemyślanego szkieletu na solidnym fundamencie (zasady procesowe), systemów doprowadzających energię i wodę (komunikacja i infrastruktura między uczestnikami postępowania) i personelu administracyjnego (uczestnicy postępowania), wreszcie materiałów budowlanych (dowodów). Dowody są zatem systemem wiążącym różnorodne składniki w jednolitą całość, natomiast pozostałe elementy tworzą nierozerwaną całość. Nawet jeśli ww. elementy pełnią różne role w utrzymaniu budynku we właściwej formie, to wydaje się, że właśnie dowodom w procesie (nie tylko zresztą karnym) przypada rola szczególna.

Mimo naukowych dociekań nie udało się znaleźć autora często powtarzanego zwrotu: „nie ma dowodu – nie ma procesu". Stwierdzenie to jest jednak niekwestionowanym dogmatem, dla każdego, kto zajmuje się problematyką postępowań sądowych. Dowody jako fundament procesu karnego od zawsze były, są i muszą być obecne na wszystkich jego etapach i stadiach.

Nie można zatem rozstrzygnąć istoty procesu karnego – kwestii zbadania odpowiedzialności karnej – bez należycie i rzetelnie przeprowadzonego postępowania dowodowego. Tak naprawdę zresztą powszechnie zwraca się uwagę na rolę subdziedziny prawa karnego procesowego, jaką stanowi prawo dowodowe, a zatem zbiór przepisów różnej rangi, które regulują i określają zarówno katalog dowodów, jak też reguły wykrywania, zabezpieczenia, pozyskiwania, przeprowadzania, wykorzystania i oceny materiału dowodowego. Jeśli na którymś z tych nie do końca precyzyjnie wyróżnianych etapów dojdzie do błędów, istnieje ryzyko, że końcowo wydane rozstrzygnięcie będzie naruszało zasady *fair trial*. Wskazane reguły mają zatem zastosowanie zarówno do tradycyjnie wyróżnianych dowodów rzeczowych czy osobowych, jak też nabierających na znaczeniu dowodów elektronicznych (dowodów cyfrowych, dowodów komputerowych, cyberdowodów, e-dowodów).

Wyróżnianie dowodów cyfrowych jest skutkiem przemian, jakie mają miejsce nie tylko w wymiarze sprawiedliwości, ale w każdej niemal dziedzinie ludzkiej egzystencji. Nie trzeba być szczególnie spostrzegawczą osobą, aby stwierdzić, że w ostatnich latach rzeczywistość, w której funkcjonujemy, zmienia się w stopniu, który jest trudny do wypowiedzenia, a co dopiero do zrozumienia. Wynalazczość w niemal dowolnej dziedzinie nie tylko promieniuje, ale wręcz w sposób niekontrolowany rozszerza się na wszelkie inne dziedziny ludzkiej aktywności. Postępująca globalizacja, rozkwit techniki informatycznej, rywalizacja międzypaństwowa, rozwój sieci Internet wraz z oszałamiającym rozprzestrzenieniem się zasięgów mediów społecznościowych, postępująca miniaturyzacja sprzętu, nowe sposoby komunikacji bezpośredniej, udostępnienie darmowych platform do tworzenia oprogramowania, a w ostatnim czasie rozwój rozmaitych aspektów uczenia się maszynowego sprawiły, że współcześnie nikt, mimo najszczerszych nawet chęci, nie może być obojętny wobec wskazanych zjawisk. Tempo przemian nastąpiło i nadal następuje w stopniu geometrycznym, co utrudnia, a wręcz uniemożliwia przemyślane oddziaływanie człowieka, a zatem również wymusza przez ustawodawcę podjęcie natychmiastowej reakcji w postaci modyfikacji lub też wprowadzenia nowych regulacji prawnych. Nie inaczej jest w przypadku prawa dowodowego, w szczególności w zakresie dowodów cyfrowych.

Przedmiotem opracowania będzie zarysowanie istotnego zagadnienia, jakie stanowi dowód cyfrowy, ale też postępowanie dowodowe z wykorzystaniem tej kategorii dowodów. Wychodząc zatem od pojęcia dowodu elektronicznego, zostaną w dalszej kolejności przedstawione specyficzne cechy, jakie posiada ten rodzaj dowodu, następnie zarysowane zostaną najważniejsze

etapy postępowania dowodowego ze szczególnym uwzględnieniem pozyskiwania i wykorzystania materiału dowodowego z perspektywy zasady swobodnej oceny dowodów (art. 7 KPK). Rozważania te nie mają zresztą i nie mogą mieć w żadnej mierze charakteru kompleksowej analizy, z uwagi na to, że problematyka postępowania dowodowego jest i powinna być przedmiotem zainteresowania niemal każdego przedstawiciela procesu karnego. Celem tego opracowania jest jednak skupienie się na specyficznej roli dowodu, który ze względu na wykorzystanie danych informatycznych dostarcza wiedzy na temat zdarzenia historycznego z udziałem sprawcy przestępstwa. Należy bowiem postawić tezę, że rozwój techniki informatycznej oraz popularność dowodów elektronicznych sprawiły, że dotychczasowa filozofia prawa dowodowego powinna ulec istotnemu przewartościowaniu. Dotyczy to w głównej mierze nie tylko przeprowadzania dowodów, ale też etapu ich oceny w celu dokonywania trafnych ustaleń faktycznych. W kontekście zatem zasady cyfryzacji procesu karnego, konieczne jest znalezienie nowej aksjologii postępowania dowodowego. Podkreślenia przy tym wymaga, że zagadnienia związane z kryminalistycznymi aspektami postępowania dowodowego zostaną postawione na marginesie rozważań.

§ 2. Definicja dowodu elektronicznego

Przepisy prawa karnego procesowego, ale też szerzej przepisy regulujące innych procedur sądowych nie regulują pojęcia dowodu elektronicznego. Z tych powodów należy odwołać się do definicji dowodu elektronicznego, jakie wypracowano w doktrynie zarówno w nauce polskiej, jak też w organizacjach związanych z rozwojem środków elektronicznych. Pojęcie „dowodu elektronicznego" (cyfrowego, e-dowodu) jest w tym zakresie przedmiotem sporów nie tylko na gruncie piśmiennictwa polskiego[1]. Jak wiadomo, wszelka definicja jest niebezpieczna, ale bez wątpienia w dobie wzrastającego wykorzystania

[1] W piśmiennictwie spotyka się z omawianego zakresu także inne określenia, takie jak: „e-dowód", „dowód IT", „dowód elektroniczny", „dowód z komputera", „dowód wygenerowany komputerowo", „wiadomość elektroniczna", „dowód pochodzący z komputera", „dowód wytworzony cyfrowo", „dowód zdigitalizowany". Obszerną literaturę dotyczącą pojęcia dowodu cyfrowego zamieszczono w publikacji *P. Lewulis*, Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym, Warszawa 2021, s. 50–85 czy *B. Oręziak*, Dowody elektroniczne a sprawiedliwość procesu karnego, Prawo w działaniu. Sprawy karne, 2020, Nr 41, s. 187–196.

dowodów elektronicznych w postępowaniu karnym zagadnienie to ma istotne znaczenie praktyczne.

Przepisy KPK nie definiują pojęcia dowodu cyfrowego, pozostawiając tę kwestię doktrynie. Choć pojęcie „dowód" jest niezwykle wieloznaczne, to w tradycyjnym podziale dowodów istotne jest kryterium źródła dowodu – którym jest osoba lub rzecz, które dostarczają środków dowodowych. Tym samym dowody mogą być osobowe i rzeczowe. Ten dychotomiczny podział został zaburzony przez dokumenty, które niekiedy traktowane są jako dowody osobowo rzeczowe[2]. Stwierdza się przy tym, że „dowód elektroniczny jest specyficznym dowodem rzeczowym. Dokonuje się fizycznego zabezpieczenia przedmiotu, natomiast dowodem jest informacja zawarta (zapisana) w tym przedmiocie"[3]. Dowód cyfrowy nie poddaje się tak łatwo klasyfikacjom, aczkolwiek powszechnie się przyjmuje, że posiada najwięcej cech dowodu rzeczowego.

Definicję dowodu cyfrowego stworzono najprawdopodobniej najwcześniej w lipcu 1998 r. wśród pracowników Naukowej Grupy Roboczej ds. Dowodów Cyfrowych (SWGDE) i brzmiała ona: „*Digital Evidence is any information of probative value that is either stored or transmitted in a binary form*" (Dowód cyfrowy to każda informacja posiadająca wartość dowodową, która jest przechowywana lub przesyłana w binarnej)[4]. Podobnie agencja rządowa USA – Narodowy Instytut Sprawiedliwości (NIJ) zajmująca się poszerzaniem wiedzy i zrozumieniem zagadnień przestępczości i wymiaru sprawiedliwości poprzez naukę definiuje dowód elektroniczny jako: „*Digital evidence is information stored or transmitted in binary form that may be relied on in court* (Informacja przechowywana lub transmitowana w formie binarnej, która może mieć znaczenie w postępowaniu sądowym)"[5].

Definicja dowodu cyfrowego wykazuje podobieństwo do pojęcia „danych informatycznych" czy „systemu informatycznego". W konwencji Rady Europy o cyberprzestępczości wskazano, że system informatyczny oznacza: „każde

[2] *J. Zagrodnik* (red.), Proces karny, Warszawa 2019, s. 339; *P. Wiliński* (red.), Polski proces karny, Warszawa 2020, s. 197 czy *P. Hofmański*, *S. Waltoś*, Proces karny, 2023, s. 363.

[3] *M. Kała*, *D. Wilk*, *J. Wójcikiewicz*, *D. Zuba* (red.), Ekspertyza sądowa, Warszawa 2023, s. 733.

[4] *C. Morgan Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence Spring 2002, vol. 1, s. 4. Na późniejszych spotkaniach grupy słowo „binarny" zostało zmienione na „cyfrowy". Wówczas przez dowody cyfrowe rozumiano przed tym dowody komputerowe, pliki: audio, pliki wideo, telefony komórkowe, cyfrowe faksy, a także oznaczenia daty wytworzenia danego pliku.

[5] https://nij.ojp.gov/digital-evidence-and-forensics, dostęp: 2.4.2024 r.

urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych" (art. 1 lit. a), natomiast przez dane informatyczne należy rozumieć „dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny".

A. Lach w pionierskiej pracy w piśmiennictwie karnoprocesowym wskazuje, że dowód cyfrowy: „Jest to informacja przechowywana lub transmitowana w formie binarnej, która może mieć znaczenie w postępowaniu sądowym"[6]. Zdaniem *B. Hołysta* z kolei przez dowód cyfrowy należy rozumieć: „informację zmagazynowaną bądź przekazaną w formacie binarnym (dwójkowym), która ma potencjalną wartość dowodową"[7]. *P. Lewulis* rozważając pojęcie dowodu cyfrowego przyjął, że „w rozumieniu szerokim są wszelkie informacje o znaczeniu dowodowym, mające pierwotnie formę danych cyfrowych i włączane do materiałów postępowania w formie wydruków lub na nośnikach danych, lecz badane i oceniane wyłącznie pod kątem ich treści bez przeprowadzenia analiz technicznych (przykładowo: przez proste uwzględnienie treści e-maila, wydrukowanych zrzutów ekranu z treścią strony internetowej, czy wydrukowanego zestawienia billingowego, które dowodzi zalogowanie się użytkownika w sieci w danym czasie). Dowodem cyfrowym w rozumieniu kryminalistycznym (*sensu stricto*) będą tylko te spośród dowodów cyfrowych, które podlegają zabezpieczeniu analizie i oceni jako dane cyfrowe z uwzględnieniem wiarygodności technicznej w oparciu o metody informatyki kryminalistycznej"[8]. Kluczowe jest zatem odróżnienie samego dowodu od nośnika danych, na którym zostaje on utrwalony. W literaturze zresztą odróżnia się dowody elektroniczne od dowodów cyfrowych, bowiem przyjmuje się, że dowód elektroniczny to dowód w pierwotnej postaci mający formę danych, natomiast dowód cyfrowy to dowód wtórny (zdigitalizowany), w którym dźwięk lub papier został przekształcony w formę cyfrową. Dowody te mają charakter dowodów rzeczowych, ponieważ zapis elektroniczny stanowi właściwość nośnika, na którym się znajduje, oraz mogą mieć charakter zarówno dowodów zmysłowych, jak i pojęciowych[9].

[6] *A. Lach*, Dowody elektroniczne w procesie karnym, Toruń 2004, s. 30.

[7] *B. Hołyst*, Kryminalistyka, Warszawa 2010, s. 758.

[8] *P. Lewulis*, Dowody cyfrowe, s. 56.

[9] *D. Jagiełło*, Przestępstwa w cyberprzestrzeni – problematyka karna i śledcza, w: *C. Banasiński* (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa 2018, s. 472.

Nawiązując do wskazanych wyżej definicji, na użytek opracowania należy przyjąć, że dowodem cyfrowym (elektronicznym) jest szczególny rodzaj dowodu rzeczowego zawierający wszelkiego rodzaju informacje (ślady cyfrowe) zapisane z wykorzystaniem systemu binarnego (zerojedynkowego), które przy wykorzystaniu odpowiedniej aparatury i oprogramowania pozwalają odtworzyć przebieg zdarzenia będącego przedmiotem postępowania niezależnie od tego, na jakim nośniku dane relewantne procesowo zostały wytworzone i gdzie są przechowywane. W praktyce śledczej zatem będą to wszelkiego rodzaju pliki (tekstowe, dźwiękowe, graficzne) oraz metadane gromadzone na dyskach lub serwerach (logi systemowe, zapisy w przeglądarce, systemie komputerowym, w sieci informatycznej w tym popularnej „chmurze"). Dowodem cyfrowym będą zatem dane pierwotnie wytworzone w systemie, jak też następczo zapisane w formie cyfrowej (zdigitalizowane) z wykorzystaniem różnych transmisji i konwersji w postaci zdjęcia, fotokopii, nagrania, skanu, printscreenu (zrzutu ekranu) i innych podobnych technik informatycznych.

Dowód cyfrowy należy jednak wyraźnie odróżnić od karnomaterialnego pojęcia dokumentu, bowiem w myśl art. 115 § 14 KK, dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne. Dowód cyfrowy nie jest również „rzeczą ruchomą ani przedmiotem w rozumieniu art. 115 § 9 KK, zgodnie z którym, rzeczą ruchomą lub przedmiotem jest także polski albo obcy pieniądz lub inny środek płatniczy, środek pieniężny zapisany na rachunku oraz dokument uprawniający do otrzymania sumy pieniężnej albo zawierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach, albo stwierdzenie uczestnictwa w spółce".

W tym kontekście warto zaakcentować, że rozwój prawa dowodowego z zakresu dowodów cyfrowych nie będzie możliwy bez ścisłej współpracy przedstawicieli doktryny procesu karnego z kryminalistykami, a zatem doskonale w tym miejscu widać mariaż przedstawicieli nauki pomocniczej, jaką jest kryminalistyka, z dogmatykami teorii prawa karnego procesowego. Można nawet pójść dalej i zaprosić do wskazanej wymiany poglądów przedstawicieli wymiaru sprawiedliwości (nie tylko organy procesowe, ale także biegłych sądowych), tak aby dzięki swojej wiedzy mogli w ramach wzajemnych interakcji i wymiany poglądów ukształtować pożądany kształt prawa dowodowego z kluczową rolą dowodów cyfrowych. Stworzenie zatem precyzyjnej i przejrzystej zarazem definicji e-dowodu czy zasad postępowania dowodowego wy-

maga bowiem ciągłej współpracy z kryminalistykami czy też przedstawicielami dyscypliny ekspertyzy sądowej z zakresu nawet informatyki sądowej.

§ 3. Pozyskiwanie dowodu elektronicznego

Z perspektywy wskazanych celów wszystkich etapów procesu karnego (art. 2 § 1 KPK), należy zwrócić uwagę, że celem postępowania jest w myśl art. 297 § 1 KPK:

1) ustalenie, czy został popełniony czyn zabroniony i czy stanowi on przestępstwo;
2) wykrycie i w razie potrzeby ujęcie sprawcy;
3) zebranie danych stosownie do art. 213 i 214 KPK;
4) wyjaśnienie okoliczności sprawy, w tym ustalenie osób pokrzywdzonych i rozmiarów szkody; oraz
5) zebranie, zabezpieczenie i w niezbędnym zakresie utrwalenie dowodów dla sądu. Wskazane reguły dotyczą również pozyskiwania dowodów cyfrowych.

W doktrynie *A. Lach* wskazuje, że dowód cyfrowy wyróżnia się na tle innych dowodów następującymi cechami, do których należy:

1) łatwość modyfikacji, a zatem jest podatny na spreparowanie lub zniszczenie;
2) łatwość w kopiowaniu do tego stopnia, że kopia równa się oryginałowi;
3) łatwość w przechowywaniu;
4) najczęściej poszlakowy charakter[10].

W podobnym tonie wypowiada się *P. Lewulis*, wymieniając następujące cechy szczególne dowodów cyfrowych:

1) wyjątkowy charakter materiału dowodowego (dowód cyfrowy może zostać przetworzony wyłącznie przy pomocy specjalistycznego systemu i oprogramowania);
2) konieczność skorzystania z pomocy biegłych przy pozyskaniu i wykorzystaniu dowodów;
3) łatwość przechowywania i ewidencjonowania;
4) łatwość modyfikacji dowodów cyfrowych i podatność na manipulację, co wymaga szczególnych umiejętności przy pozyskiwaniu dowodów;

[10] *A. Lach*, Dowody elektroniczne, s. 32–33.

5) trwałość dowodów cyfrowych (można przechowywać dowody przez wiele lat pod warunkiem, że są odpowiednio zabezpieczone); oraz
7) łatwość wykonania kopii, która jest identyczna z oryginałem[11].

Aktualnie obowiązujące przepisy w niewielkim zakresie regulują problematykę postępowania z cyfrowym materiałem dowodowym, pozostawiając tę kwestię praktyce oraz przepisom wewnętrznym[12]. Zresztą nawet w aktach rangi podustawowej w tym zakresie ograniczono się głównie do określenia ramowych zasad ewidencji tej szczególnej kategorii dowodów.

Przepisy KPK z kolei w dziale V (ani też nigdzie indziej) nie regulują problematyki pozyskiwania dowodów elektronicznych, a także ich późniejszego wykorzystywania. W tym zakresie zatem znajdą zastosowanie ogólne przepisy dotyczące czynności poszukiwawczych: zatrzymanie nośników, na których utrwalono wskazane dowody (art. 217 KPK), przeszukanie (art. 219 i n. KPK), a także przepisy o kontroli i utrwalaniu rozmów (art. 237 i n. KPK). Z perspektywy dowodów cyfrowych istotne znaczenie miała regulacja art. 218 KPK, a zatem urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celno-skarbowe oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i 180d PrTelekom, jeżeli mają znaczenie dla toczącego się postępowania. Podobnie kluczowe jest także wskazane w art. 218a KPK zabezpieczenie danych przez urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną lub świadczące usługi drogą elektroniczną oraz dostawcy usług cyfrowych, którzy są obowiązani są niezwłocznie zabezpieczyć, na żądanie sądu lub prokuratora zawarte w postanowieniu, na czas określony, nieprzekraczający jednak 90 dni, dane informatyczne przechowywane w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym. Uwzględniając przepisy rozdziału 25 KPK o przeszukaniu i zatrzymaniu, należy mieć na względzie, że stosownie do treści art. 236a KPK przepisy tego rozdziału stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie

[11] *P. Lewulis*, Dowody cyfrowe, s. 65–68.

[12] Tak przykładowo zarządzenie Nr 4 KGP z 9.2.2017 r. w sprawie niektórych form organizacji i ewidencji czynności dochodzeniowo-śledczych Policji oraz przechowywania przez Policję dowodów rzeczowych uzyskanych w postępowaniu karnym (Dz.Urz. KGP z 2017 r. poz. 9).

albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.

Wydaje się zatem, że pożądane jest, a wręcz niezbędne, wprowadzenie do przepisów działu V KPK pt. „Dowody" regulacji dotyczącej definicji dowodu cyfrowego z wykorzystaniem propozycji formułowanych w literaturze przedmiotu. Wskazane regulacje powinny mieć zatem zastosowanie zarówno do etapu postępowania przygotowawczego, jak też postępowania jurysdykcyjnego. Nowe przepisy powinny precyzować metody zabezpieczania i przeprowadzania dowodów cyfrowych metod dokumentacji czynności procesowych. Jeśli zatem zostaną uchwalone wskazane zapisy, to prawdopodobnie dojdzie do zmiany sposobu postrzegania dyrektyw wynikających ze swobodnej oceny dowodów, zarówno z perspektywy „wskazań wiedzy", jak i „doświadczenia życiowego". Wszystko to prowadzi do wniosku, że nie tylko organy procesowe (Policja, prokuratura, sąd), ale także strony i reprezentanci stron procesowych (obrońcy i pełnomocnicy) będą zmuszeni wzbogacić swoją wiedzę z zakresu dowodów cyfrowych. Jeśli tego nie uczynią, zgodnie z wymogami prakseologicznego ciężaru dowodu zwiększy się ryzyko popełnienia przez nich omyłek sądowych lub zaniedbania obowiązków procesowych.

Należy zwrócić uwagę, że pojęcie dowodów cyfrowych ma znaczenie nie tylko teoretyczne, ale również fundamentalne znaczenie praktyczne z perspektywy czynności procesowych związanych z przeszukaniem, zatrzymaniem rzeczy w celu zastosowania tymczasowego zajęcia mienia ruchomego (art. 295 KPK), czy zabezpieczenia majątkowego (art. 291 KPK). Dowodem tego są chociażby dwie uchwały SN wydane na gruncie przepisów pozakodeksowego prawa karnego. W pierwszej z uchwał SN wskazał, że środki zgromadzone na rachunku bankowym nie mają cech dowodu rzeczowego w rozumieniu art. 86 ust. 13 TerroryzmU, gdyż „nie istnieją jako rzeczy, a są wyłącznie zapisami w systemie informatycznym, (...) dowód rzeczowy w procedurze karnej, zawsze ma więc cechy indywidualne, gdyż każdy niesie ze sobą konkretne informacje ważne dla przebiegu procesu – jest bowiem źródłem dowodowym. Istotą wszak przeprowadzania dowodu w procesie sądowym jest dokonywanie wnioskowań w oparciu o ten konkretny dowód, które prowadzą do dokonywania ustaleń w zakresie faktów. (...) środki zgromadzone na rachunku bankowym nie mają tych cech, gdyż nie istnieją jako rzeczy – przedmioty, są wyłącznie zapisami w systemie informatycznym. Zapisem informatycznym, któremu nie odpowiada żaden konkretny przedmiot – banknot, który mógłby zostać poddany oględzinom. Tak więc środki te w ogóle nie mają cech dowodu

w znaczeniu procesowym"[13]. W drugiej z uchwał SN[14] stwierdził, że zgromadzone na rachunku bankowym środki nie są dowodem rzeczowym, o którym mowa w art. 106a ust. 8 PrBank. Ustawodawca zresztą zdawał sobie sprawę, że mogą powstać mimo to wątpliwości w praktyce stosowania przepisów o przeszukaniu i zabezpieczeniu majątkowym. Nie przytaczając szczegółowej argumentacji, w obu orzeczeniach SN słusznie dokonał odróżnienia specyfiki dowodu cyfrowego od dowodu rzeczowego. Dowodem rzeczowym będą zatem wyciągi z rachunków, potwierdzenia wypłat, nagrania z kamer przy dokonywaniu wpłat czy wreszcie banknoty wpłacone przez daną osobę, ale już nie banknoty wypłacone w banku jako równowartość zapisów cyfrowych w systemie. Banknot papierowy może być zatem dowodem rzeczowym jako nośnik określonej informacji przydatnej z perspektywy przedmiotu postępowania, nie zaś jako miernik wartości pieniądza. Ustawodawca niestety nie dostrzegając specyfiki czynności przeszukania, z dniem 1.7.2019 r. dodał w rozdziale 25 pt.: „Zatrzymanie rzeczy. Przeszukanie" nowy art. 236b KPK, który stanowi, że: „§ 1. Rzeczą lub przedmiotem w rozumieniu przepisów niniejszego rozdziału są również środki na rachunku. § 2. Postanowienie w przedmiocie dowodów rzeczowych może dotyczyć środków na rachunku, jeżeli zostały zatrzymane jako dowód w sprawie". Jego wprowadzenie do przepisów KPK może powodować ryzyko nadużywania częstotliwości nieuzasadnionego zatrzymania przedmiotów i liczby nieuzasadnionych zabezpieczeń majątkowych jako środków wymuszania czynności procesowych.

Z uwagi na podatność dowodów elektronicznych na zniszczenie lub kontaminację wszelkie czynności regulujące pozyskiwanie materiału cyfrowego wymagają dokonania z niezwykłą starannością zgodną ze wskazaniami kryminalistyki, a w szczególności informatyki śledczej. Organy postępowania karnego z udziałem pomocników organów procesowych powinny dokonać odpowiednich kopii materiałów zgromadzonych na nośnikach, wykonania kopii binarnych[15]. Niewłaściwe przeprowadzenie czynności może skutkować uszkodze-

[13] Uchw. SN z 13.10.2021 r., I KZP 1/21, OSNKW 2021, Nr 11–12, poz. 42. Wraz z krytycznymi glosami *M. Kurowskiego*, Prok. i Pr. 2022, Nr 2, s. 131 i n. oraz *J. Dużego*, Prok. i Pr. 2022, Nr 4, s. 157.

[14] Uchw. SN z 9.11.2021 r., I KZP 3/21, OSNK 2022, Nr 1, poz. 3.

[15] Zob. *M. Chrabkowski*, *K. Gwizdała*, Zabezpieczenie dowodów elektronicznych, Prok. i Pr. 2015, Nr 12, s. 164–178; *P. Karasek*, Odzyskiwanie usuniętych dowodów cyfrowych w postępowaniu karnym, Prok. i Pr. 2016, Nr 7–8, s. 100–120; *P. Lewulis*, Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych, Prok. i Pr. 2022, Nr 3, s. 119–147.

niem, zniszczeniem lub obniżeniem wiarygodności zebranych śladów cyfrowych.

§ 4. Wykorzystanie e-dowodu z perspektywy zasady swobodnej oceny dowodów

Procedura wykorzystania wskazanej kategorii dowodów również nie została uregulowana w sposób precyzyjny. Tym samym znajdują zastosowanie ogólne reguły przeprowadzania dowodów. Inicjatywę dowodową zatem posiadają strony, ale organy postępowania mogą dopuścić dowód z urzędu (art. 167 KPK). Chociaż przepisy tego nie regulują, podkreślenia przy tym wymaga, że w przypadku wniosku dowodowego konieczne jest wyraźne oznaczenie okoliczności, która powinna być udowodniona (art. 169 KPK), co w praktyce nie jest łatwe w przypadku czynności przeszukania. Wniosek dowodowy, który nie spełnia wymogów ustawowych, powinien zostać oddalony (art. 170 KPK).

Niejednolity charakter dowodu cyfrowego, będącego szczególnym rodzajem dowodu rzeczowego, nie pozwala jednoznacznie wskazać, w jaki sposób należy go przeprowadzić w toku postępowania przygotowawczego lub w postępowaniu jurysdykcyjnym. Mając na względzie problematykę w ogóle dowodu z dokumentu i pomijając szczególne sytuacje, należy stwierdzić, że przeprowadzenie dowodu cyfrowego powinno nastąpić w drodze oględzin (art. 207 § 1 KPK), eksperymentu procesowego (art. 211 KPK) czy też opinii biegłego (200 KPK). Niekiedy jednak taki dowód może zostać przeprowadzony w trybie odczytania (art. 393 KPK), a częściej w formie odtworzenia (art. 393a KPK). Każda z tych czynności wymaga sporządzenia osobnego protokołu (art. 143 KPK).

Tym samym należy wskazać, że sposób przeprowadzania dowodu elektronicznego powinien zależeć od rodzaju danego dowodu, a ściślej sposobu jego utrwalenia. Nagranie przebiegu zdarzenia, czy to w postaci obrazu dźwięku (plik mp3) czy też obrazu i dźwięku (np. plik mp4), powinno zostać odtworzone na rozprawie, w takim zakresie w jakim podmiot wskazał we wniosku dowodowym (art. 169 KPK) na zasadach przyjętych w art. 393a KPK.

Nie ma znaczenia, czy będzie to dokument urzędowy (art. 393 § 1 KPK) czy tzw. dokument prywatny (art. 393 § 3 KPK). Przypomnieć należy, że zgodnie z art. 393 § 3 KPK mogą być odczytywane na rozprawie wszelkie dokumenty

prywatne, powstałe poza postępowaniem karnym, w szczególności oświadczenia, publikacje, listy oraz notatki. Odczytywanie *sensu largo*, o którym mowa w art. 393 § 1 lub § 3, lub art. 393a KPK, rozumiane jako werbalizacja treści zamieszczonej w dokumencie elektronicznym występuje także w odniesieniu do dokumentów pozyskanych w formie cyfrowej (np. treść SMS, bloga, treść strony WWW, wpisu w serwisie społecznościowym, nagranie oświadczenia na platformie streamingowej YouTube). Odczytaniu lub uznaniu za ujawnione bez odczytywania będą podlegać zatem także treści takie jako logi, wpisy w przeglądarce, autouzupełnienia w formularzu.

Oględziny treści cyfrowej będą właściwe co do zasady w odniesieniu do treści graficznych (np. wiadomość MMS, plik graficzny, obrazek, zdjęcie, wykres, schemat analizy kryminalnej, internetowy mem, mapa, komiks itp.), będą co do zasady podlegać oględzinom w trybie art. 207 § 1 KPK. W praktyce przeprowadza się dowód z nagrania pliku graficznego oraz pliku zawierającego monitoring wideo, dzieląc plik wideo na zestawienie obrazów (*quasi*-slajd *show*), a każdy z tych obrazów zostaje następnie opisany, co w aktach sprawy dokładnie znajduje się na wydruku danej klatki filmowej (*screen*). Tym samym plik wideo w toku wykorzystania materiału dowodowego staje się dokumentem, zamieniającym dźwięk lub obraz na tekst. Tak stworzone zestawienie plików graficznych może z kolei podlegać dodatkowo odczytaniu w trybie art. 393 § 1 lub art. 393 § 3 KPK.

W orzecznictwie wskazuje się w kontekście procedury przeprowadzania dowodów cyfrowych – najczęściej w formie odtwarzania plików audio oraz wideo. Sąd Najwyższy wskazał wielokrotnie, że konieczne jest wnikliwe ich przeprowadzenie w drodze czynności odczytania w toku rozprawy lub też zasięgnięcia opinii biegłego z zakresu informatyki. Sąd Najwyższy stwierdził, że „Nie można inaczej «odtworzyć» zapisów cyfrowych na nośniku informacji – jak w drodze zwykłego odtworzenia (odczytania zapisów cyfrowych z nośnika w czasie rozprawy) zapisów z płyty, albo, gdy nośnik jest uszkodzony, korzystając z opinii biegłego z zakresu informatyki, albowiem tylko ten biegły może odczytać zapisy na uszkodzonym nośniku”[16].

Wskazuje się w doktrynie, że niezwykle istotne jest, aby dowody cyfrowe zostały udostępnione stronom, a w szczególności w toku ich prezentowania należy:

1) zapewnić równe szanse zapoznania się z dowodami cyfrowymi, w szczególności w przypadku stron biernych (podejrzanego i oskarżonego);

[16] Post. SN z 24.10.2017 r., V KK 140/17, Legalis.

2) zagadnienia techniczne należy przedstawiać w sposób przystępny i wykorzystywać schematy, animacje i połączenia w komunikacji między podmiotami;
3) umożliwiać weryfikację autentyczności przedstawionego materiału dowodowego; oraz
4) zapewniać integralność danych z perspektywy zasady szybkości postępowania i ekonomiki procesowej w toku prezentowania dowodów[17].

Obserwacja praktyki organów postępowania karnego dowodzi, że mają one bezpośrednią styczność z dowodami cyfrowymi nie tylko w przypadkach przestępstw przeciwko ochronie informacji, ale wszędzie tam, gdzie zostaje utrwalony przebieg zdarzenia przestępnego. Chociaż nie ma w Polsce obszernych badań na temat częstotliwości wykorzystania dowodów cyfrowych w postępowaniu sądowym[18], to w piśmiennictwie zresztą wskazuje się słusznie, że z uwagi na wzrost liczby danych gromadzonych przez organy ścigania, a także postęp technologiczny skutkujący coraz szybszymi komputerami, nieuchronnie rozszerza się możliwość wykorzystania komputerów w kryminalistyce, czego przejawem jest: komputeryzacja kartotek, wykorzystanie komputerów do wykonywania ekspertyz, analiza danych i wspomaganie procesu decyzyjnego, komputery operacyjno-dyżurujące oraz komputerowe systemy zabezpieczania ważnych obiektów[19].

Twierdzi się zresztą w piśmiennictwie *explicite*, że „Ślady zjawiskowe (cyfrowe, magnetyczne i inne) to także «rzeczy» jako rzeczowe źródła dowodu niesubstancjalnego, mimo że nie podlegają oględzinom bezpośrednim, lecz wymagają ekspertyzy i sformułowania na ich podstawie opinii biegłego. Na tle wykładni ogółu przepisów k.p.k. prawnicze pojęcie rzeczy jako źródła dowodu rzeczowego zarówno zmysłowego jak i pojęciowego (dokument jest również «rzeczą»), ma zatem zakres szerszy niż rzecz w prawie cywilnym i niż sta-

[17] *A. Lach*, Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne, E-Biuletyn 2004, Nr 2, s. 8.

[18] Potwierdzają to świetnie przeprowadzone badania w zakresie wykorzystania dowodów cyfrowych w postępowaniu karnym w pracy *P. Lewulis*, Gromadzenie, s. 135–142, gdzie w 370 postępowaniach w sprawach zakończonych prawomocnym orzeczeniem w latach 2016–2018 dotyczących art. 255, 256 KK, art. 116 PrAut, art. 267 i n. oraz art. 286 i 287 KK wskazano, że dowody cyfrowe wystąpiły w 253 sprawach (zatem 68,3%) niezależnie od tego, czy sprawca posługiwał się technologią informatyczną.

[19] *G. Dobrowolski*, *W. Filipkowski*, Charakterystyka informatyki kryminalistycznej w Polsce w ujęciu teoretycznym, w: V. *Kwiatkowska-Wójcikiewicz*, *D. Wilk*, *J. Wójcikiewicz*, Kryminalistyka a nowoczesne technologie, Kraków 2019, s. 313–316.

nowi o tym art. 173 § 1 lub art. 207 § 1 KPK"[20]. Słusznie się bowiem wskazuje w orzecznictwie, że „Słowne przekłady (tzw. stenogramy) zapisów utrwalonych na nagraniach rozmów nie mogą zostać wprowadzone do procesu jako dowód samoistny, a jedynie jako załącznik – uzupełnienie dowodu pierwotnego, którym bez wyjątku pozostają utrwalone na nagraniach zapisy dźwiękowe. Dlatego też nie można czynności zaliczenia w poczet dowodów zapisu dźwiękowego rozmów przez odsłuchanie (odtworzenie) albo bez odsłuchania, zastępować odczytaniem stenogramów"[21]. Sąd Najwyższy zresztą docenia wagę dowodów elektronicznych, podkreślając, że „Informatyka śledcza to dziedzina dynamicznie rozwijająca się, co tym bardziej obliguje organy wymiaru sprawiedliwości do dążenia do uzyskiwania wiedzy o jak najdoskonalszych metodach zabezpieczania dowodów w sprawie (...) Z uwagi na specyfikę danych elektronicznych (informatycznych), które na równi z innymi dowodami są podstawą wyrokowania, ich ocena musi być niezwykle ostrożna, gdyż doświadczenie życiowe każdego użytkownika sprzętu komputerowego wskazuje, że statystycznie bardzo często dane te ulegają modyfikacjom"[22]. Przyszłość sprawnego postępowania karnego będzie zależała od sposobu wdrożenia naczelnej zasady procesowej, jaką jest zasada cyfryzacji[23]. Im większe będzie oddziaływanie technologii cyfrowej na proces karny, tym proces karny będzie w wyższym stopniu bliski modelowi optymalnemu: wydaniu trafnego rozstrzygnięcia z poszanowaniem praw i wolności obywatelskich, unikając przy tym zbędnej zwłoki w postępowaniu.

§ 5. Rola biegłego w zakresie dowodzenia z wykorzystaniem dowodów cyfrowych

W przypadku dowodów cyfrowych niezwykle częste będzie powołanie biegłych sądowych lub pracowników organów ścigania, gdyż z reguły weryfikacja autentyczności dowodu cyfrowego będzie wymagała znajomości zasad i technik postępowania z materiałem cyfrowym. Rola wskazanych osób nie ograni-

[20] *R. Kmiecik*, Rzeczy, ślady i dokumenty jako przedmiot postanowienia prokuratora „co do dowodów rzeczowych" (art. 323 § 1 k.p.k.), Prok. i Pr. 2022, Nr 7–8, s. 47.

[21] Post. SN z 12.3.2020 r., V KK 8/20, Legalis.

[22] Wyr. SN z 20.6.2013 r., III KK 12/13, Legalis.

[23] Zob. *P. Czarnecki*, Zasada elektronizacji (cyfryzacji) procesu karnego, w: *D. Szumiło-Kulczycka* (red.), W pogoni, s. 439–448.

cza się wyłącznie do pozyskiwania, zabezpieczania śladów cyfrowych, ale mają istotne znaczenie z perspektywy wizualizacji zebranych danych z wykorzystaniem analizy kryminalnej.

Zgodnie z art. 193 § 1 KPK, jeżeli stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych, zasięga się opinii biegłego albo biegłych, natomiast w myśl art. 193 § 2 KPK, w celu wydania opinii można też zwrócić się do instytucji naukowej lub specjalistycznej. Należy przyjąć ogólną dyrektywę interpretacyjną, która ustanawia domniemanie wzruszalne, że w przypadku dowodów cyfrowych regułą będzie korzystanie z pomocy biegłego. Sąd Najwyższy przyjął, że „Zarówno dyspozycja art. 7 KPK, jak i art. 193 § 1 KPK nie zakazuje sądowi czynienia własnych ustaleń obejmujących jakiekolwiek wiadomości ze sfery techniki, czy działania urządzeń. Domeną biegłych są «wiadomości specjalne», a więc takie wiadomości faktyczne czy praktyczne, które wykraczają poza przeciętne umiejętności czy wiedzę. Wiedza dostępna dla dorosłego człowieka o odpowiednim doświadczeniu życiowym i wykształceniu (...) może natomiast zostać zastąpiona wiedzą i doświadczeniem sędziowskim”[24].

Sąd Najwyższy wskazał przykładowo, że „Nawet zakładając, że rozpoznający sprawę sędzia sądu *ad quem* orientował się w stopniu ponadprzeciętnym w problematyce logowania się telefonów i azymutów, za pomocą których doszło do tego logowania, to i tak zobligowany był skorzystać z dowodu z opinii biegłego, co jasno wynikało z treści art. 193 § 1 KPK”[25]. Nie sposób jednak uznać, że każdorazowe zbadanie dowodu cyfrowego będzie wymagać ustaleń dokonanych przez biegłego. Przykładowo SN wskazał, że „Ustalenia odnośnie osoby biorącej udział w zarejestrowanej rozmowie telefonicznej mogą być poczynione w oparciu o każdy miarodajny w tym zakresie dowód. Nie jest zarazem tak, aby to wyłącznie opinia biegłego z zakresu fonoskopii mogła stanowić podstawę ustaleń faktycznych w tym zakresie”[26].

Jeżeli ustalenie danego faktu nie wymaga wiedzy specjalnej, to wystarczające jest odwołanie się do zasad swobodnej oceny dowodów zgodnie z kryteriami wskazanymi w art. 7 KPK. Należy bowiem pamiętać, że to rolą organu procesowego (Policji, prokuratora, sądu) jest dokonywanie oceny wiarygodności dowodu cyfrowego, natomiast opinie biegłych, dowody rzeczowe

---

[24] Post. SN z 10.2.2021 r., IV KK 574/20, Legalis, w którym nawiązano do słynnego wyr. SN z 15.4.1976 r., II KR 48/76, OSNKW 1976, Nr 10–11, poz. 133 dotyczącego rozumienia wiadomości specjalnych.

[25] Wyr. SN z 9.9.2020 r., IV KK 155/19, Legalis.

[26] Post. SN z 26.6.2019 r., V KK 298/19, Legalis.

czy osobowe mogą być pomocne w przypadku dodatkowej weryfikacji ustaleń wynikających z dowodu cyfrowego. Przykładowo zatem nie będzie wymagane powołanie biegłego z zakresu informatyki, jeśli organ postępowania otrzymał od operatora bilingi telefoniczne zawierające wykaz numerów telefonów, czas i kierunek rozmów czy nawet lokalizatory czasu i miejsca logowania się określonych numerów telefonów w stacjach bazowych (tzw. BTS). Należy przyjąć ogólną dyrektywę postępowania, w myśl której dopóki strona nie kwestionuje autentyczności dowodu cyfrowego, nie będzie konieczne zasięgnięcie pomocy biegłego. Dotyczy to przykładowo sytuacji, gdy w aktach sprawy są zdigitalizowane wydruki z komunikatorów internetowych, forów internetowych czy mediów społecznościowych.

Dowody cyfrowe zatem podlegają ocenie na zasadach ogólnych, w głównej mierze więc zastosowanie znajdzie art. 7 KPK, zgodnie z którym organy postępowania kształtują swe przekonanie na podstawie wszystkich przeprowadzonych dowodów, ocenianych swobodnie z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego. Wskazana zasada „wyznacza dyrektywę postępowania zakazującą przyjęcie określonego systemu oceny dowodów. System ten opiera się na odrzuceniu przyjętego *a priori* rodzajowego wartościowania dowodów, ich generalnego podziału na lepsze czy gorsze, bardziej czy mniej wartościowe, na obowiązku każdorazowej oceny wszystkich zgromadzonych dowodów”[27]. Swobodna ocena dowodów oznacza, że „organ procesowy, a zwłaszcza sąd, ocenia dowody i wyciąga z nich wnioski według swego przekonania, nie będąc skrępowany w tym przedmiocie regułami dowodowymi, jednak z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego”[28]. Specyfika dowodów cyfrowych prowadzi do wniosku, że w głównej mierze mają charakter dowodów poszlakowych, czyli dotyczących faktu ubocznego. Taka sytuacja dotyczy przykładowo informacji o logowaniu się w określonej lokalizacji, wizerunku sprawcy utrwalonego na monitoringu miejskim czy też wpisywania określonych zwrotów czy fraz w przeglądarce internetowej. Oznacza to, że z reguły konieczne będzie dla skazania wykorzystanie dowodów bezpośrednich, a zatem dotyczących faktu głównego.

Z przedstawionych powyżej rozważań jednoznacznie wynika, że zasada swobodnej oceny dowodów zabrania formułowania zamkniętego katalogu do-

[27] *S. Waltoś*, *P. Hofmański*, Proces karny, 2023, s. 268; *P. Wiliński* (red.), Polski proces karny, s. 336.

[28] *J. Zagrodnik* (red.), Proces karny, 2019, s. 112.

wodów. Tym samym ustawodawca, a może jedynie tylko orzecznictwo lub doktryna, będą zmuszeni sformułować zarówno nowe kryteria dopuszczalności pozyskiwania dowodów, jak też jeszcze bardziej wykorzystania dowodów do dokonania ustaleń faktycznych.

Na gruncie postępowania cywilnego SA w Krakowie badając wiarygodność wydruku treści strony internetowej w zakresie naruszenia praw autorskich, stwierdził, że: „Zrzut ekranu jest utrwaleniem obrazu wyświetlanego w danej chwili na ekranie monitora w pliku, który to plik, wraz z zapisaną informacją o obrazie daje się edytować przy użyciu dostępnych powszechnie narzędzi do obróbki grafiki. Oczywista jest możliwość edytowania pliku, co pozwala na przyjęcie, że zrzut z ekranu może podlegać modyfikacjom. Istnieją możliwości zabezpieczenia pod względem dowodowym zaobserwowanej treści strony internetowej w taki sposób, by nie budziło wątpliwości, iż nie doszło do żadnej modyfikacji obrazu, widocznego w danej chwili na ekranie komputera (np. stosowany często protokół notarialny, odpowiednie zapisanie treści strony do pliku). Sąd nie ma obowiązku dopuszczać dowodu w postaci niepotwierdzonego wydruku strony internetowej, a nawet jeśli tak uczyni, to sam oceni jego moc dowodową. Sąd może zarządzić badanie takiego środka dowodowego z udziałem biegłych, treść strony internetowej można udowadniać przy pomocy wszelakich środków dowodowych, jednakże wymaga to stosownych wniosków dowodowych pochodzących od strony, która chce dowodzić swoich racji na podstawie np. zrzutu ekranowego”[29]. Nie jest to zresztą specyfika postępowania cywilnego, bowiem coraz częściej (w szczególności w sprawach z oskarżenia prywatnego o znieważenie z art. 212 KK i zniesławienie z art. 216 KK) podmioty prywatne gromadzące dowody, mając na względzie wiarygodność wskazanego materiału dowodowego i zdając sobie sprawę, że obraz strony jest dynamiczny, uzyskują u notariusza zaświadczenie o odczytaniu treści strony internetowej. Także ta okoliczność wskazuje, że istnieje potrzeba zmian w zakresie dokumentacji treści internetowych.

§ 6. Podsumowanie

W konkluzjach warto odpowiedzieć nie tylko na pytania sformułowane we wstępie, ale też należy podzielić się refleksjami wynikającymi z lektury tekstu. Poniżej zatem kilka spostrzeżeń, które stanowią próbę syntetycznego uję-

[29] Wyr. SA w Krakowie z 15.6.2016 r., I ACa 315/16, Legalis.

cia omawianego zagadnienia. Niniejsze wnioski powinny zatem stanowić zarazem punkt wyjścia dla przyszłych badaczy do pogłębionej analizy problematyki dowodów cyfrowych nie tylko w zakresie pozyskiwania i wykorzystywania ich w postępowaniu karnym.

Po pierwsze, chociaż brakuje danych, analiz, ale też badań naukowych na temat przyszłości prawa dowodowego, to jednak w kontekście wydaje się zasadne postawienie tezy, że niezależnie od modelu procesu karnego w danym państwie to dowody cyfrowe, jako *sui generis* rodzaj dowodu rzeczowego, będą wyznaczać kierunek rozwoju prawa dowodowego nie tylko w postępowaniu karnym, ale też w innych postępowaniach mających na celu zbadanie kwestii odpowiedzialności prawnej. Pamiętać bowiem należy, że dowody cyfrowe występują nie tylko w przypadku przestępstw popełnianych przy wykorzystaniu narzędzi, systemów i sieci informatycznych, ale też przestępczości pospolitej, w której przebieg zdarzeń przestępczych został utrwalony w postaci śladów informatycznych. Nie będzie zatem przesadą stwierdzenie, że przyszły proces karny musi być procesem, w którym będą rządzić właśnie e-dowody.

Po drugie, obserwując zjawisko zwiększenia się udziału przestępstw z wykorzystaniem nowoczesnej technologii informatycznej, a w szczególności cyberprzestępczości można zauważyć, trwający wyścig między organami ścigania a sprawcami popełniającymi przestępstwa przy użyciu osiągnięć rewolucji cyfrowej. Bez rozwoju infrastruktury informatycznej, podniesienia wiedzy i doświadczenia wśród organów ścigania nie będzie zatem możliwe skuteczne zwalczanie zorganizowanej przestępczości transgranicznej czy też międzynarodowej, nie mówiąc już o zwalczaniu przestępstw popełnianych z wykorzystaniem sieci informatycznych. Obserwując rozwój struktur, zadań, ale też funkcjonowanie Biura Bezpieczeństwa w Ministerstwie Sprawiedliwości, jak również działalność Centralnego Biura Zwalczania Cyberprzestępczości, można stwierdzić, że osoby odpowiedzialne za wymiar sprawiedliwości w sprawach karnych doskonale zdają sobie sprawę, iż konieczne jest wdrożenie spójnej polityki zwalczania cyberprzestępczości, a nie można tego zrobić bez właściwego pozyskania, zabezpieczenia i wykorzystania dowodów cyfrowych.

Po trzecie, w ramach współpracy międzynarodowej, ale też w ramach współpracy państw członkowskich Unii Europejskiej dostrzegalne są problemy związane ze wzrastającą cyberprzestępczością i praktycznymi problemami związanymi ze sprawnym gromadzeniem materiału dowodowego w postaci cyfrowej. Proces ten zresztą postępuje od kilku lat, a rozwój techniki sprawia, że konieczne jest nie tylko tworzenie nowych rozwiązań prawnych, ale też prowadzenie badań naukowych w zakresie nowych technologii informa-

tycznych. Odpowiedzią na to jest konieczność zacieśnienia współpracy w zakresie nie tylko wzajemnego uznawania dowodów, ale też tworzenia standardów cyberprawa dowodowego. W tym zakresie niezbędne jest wspólne zaangażowanie zarówno osób zarządzających wymiarem sprawiedliwości, jak też zaproszenie do współpracy biegłych sądowych, przedstawicieli nauk pomocniczych procesu karnego (kryminalistyka, analiza kryminalna, ekspertyza sądowa), w celu wypracowania aktów normatywnych gwarantujących sprawne ściganie karne i równocześnie spełniających standard rzetelnego procesu karnego.

Po czwarte, należy postulować w przepisach ogólnych (dział I), zamieszczenie legalnej definicji zasady cyfryzacji (elektronizacji) procesu karnego, co będzie miało kluczowe znaczenie z perspektywy rekonstrukcji modelu przyszłego procesu karnego i także pozwoli w istotnym zakresie interpretować przepisy o dowodach elektronicznych. Tym samym w dziale V „Dowody" należy zamieścić ogólne przepisy regulujące definicję dowodu elektronicznego, ogólne zasady zabezpieczania materiałów cyfrowych, sporządzania ich duplikatów (odpisów, kopii) dla uczestników postępowania karnego oraz ich wykorzystywania w toku dokonywania ustaleń faktycznych. Wydaje się, że aktualne sposoby przeprowadzania dowodów rzeczowych w formie oględzin lub też dokumentów na zasadach ogólnych nie są wystarczające.

Po piąte, mimo licznych zalet dowodów elektronicznych (łatwa dostępność, błyskawiczne przetwarzanie i wyszukiwanie informacji, bezproblemowe udostępnianie dla uczestników procesu, oszczędność kosztów postępowań, ułatwienia w zakresie analizy) szerokie korzystanie z dowodów elektronicznych niesie ze sobą wiele niebezpieczeństw. Nawet zatem niepoprawni optymiści w zakresie popularyzacji dowodów elektronicznych są świadomi mankamentów e-dowodów. W przypadku tej kategorii dowodów występuje bowiem wiele wad, do których z całą pewnością należy: wciąż trudna do określenia podatność na kontaminację, kosztochłonność w prawidłowym zabezpieczaniu przed utratą lub zniekształceniem, konieczność nakładów finansowych na szkolenia pracowników oraz zakup aparatury i oprogramowania, trudności poznawcze, problemy z autoryzacją i autentycznością dowodów czy wreszcie brak standardów dowodzenia w procesie cyfrowym. O tych czynnikach nie można zapominać, tworząc nowoczesny proces karny, nawet jeśli zostaną podjęte starania w celu minimalizacji niniejszych zagrożeń dla rzetelnego procesu karnego.

Po szóste wreszcie, mając zatem na względzie swoisty rachunek zalet i wad dowodów elektronicznych, jesteśmy skazani nie tyle na w pełni cyfrowy pro-

ces karny, lecz raczej na poszukiwanie przysłowiowego „złotego środka" na osi modelu procesu karnego. Konieczne jest zatem stopniowe wprowadzanie dowodów cyfrowych w celu znalezienia punktu równowagi między tradycyjnym (papierowym) procesem karnym a jego alternatywną postacią w postaci binarnego procesu karnego. O tym, gdzie punkt określić, zadecyduje nie tyle legislator czy tempo rewolucji cyfrowej, ile rzeczywistość w codziennej pracy organów ścigania oraz ich przyzwyczajenie do tradycyjnych form czynności procesowych. Jedno jest pewne, że z biegiem czasu na wskazanej osi będziemy przesuwać się w kierunku cyfryzacji procesu karnego.